

**In the Matter of:**  
**PrivacyCon Workshop**

*January 14, 2016*  
*Final Version*

**Condensed Transcript with Word Index**



For The Record, Inc.  
(301) 870-8025 - [www.ftrinc.net](http://www.ftrinc.net) - (800) 921-5555

1

1 UNITED STATES OF AMERICA  
 2 FEDERAL TRADE COMMISSION  
 3  
 4 PRIVACYCON WORKSHOP  
 5  
 6 THURSDAY, JANUARY 14, 2016  
 7  
 8 FEDERAL TRADE COMMISSION  
 9 Constitution Center  
 10 400 Seventh Street, S.W.  
 11 Washington, DC  
 12  
 13  
 14  
 15  
 16  
 17  
 18  
 19  
 20  
 21  
 22  
 23  
 24  
 25

3

1 P R O C E E D I N G S  
 2 - - - - -  
 3 MS. YEUNG: Good morning and welcome to  
 4 PrivacyCon. I am Tina Yeung, a paralegal in the FTC's  
 5 Office of Technology, Research, and Investigation, or  
 6 OTech. Before we commence, I have some brief  
 7 housekeeping details to run through with you.  
 8 First, if you could please silence any mobile  
 9 phones and other electronic devices.  
 10 Second, if you leave the building during the  
 11 event, you will have to come back through security.  
 12 Please bear this in mind, especially if you're  
 13 participating on a panel so you don't miss it.  
 14 Most of you received an FTC lanyard at  
 15 registration. We reuse these, so please return your  
 16 badge to our event staff when you leave today.  
 17 If an emergency occurs that requires you to  
 18 leave the conference center but remain in the building,  
 19 follow the instructions provided over the PA system. If  
 20 an emergency occurs that requires the evacuation of the  
 21 building, an alarm will sound. Everyone should leave  
 22 the building through the main 7th Street exit, turn left  
 23 and assemble across E Street. Please remain in the  
 24 assembly area until further instruction is given.  
 25 If you notice any suspicious activity, please

2

1 I N D E X  
 2  
 3 REMARKS PAGE  
 4 By Chairwoman Ramirez 5  
 5 By Commissioner Brill 130  
 6 By Professor Cranor 314  
 7  
 8 SESSION PAGE  
 9 Session 1: The Current State of  
 10 Online Privacy 14  
 11 Session 2: Consumers' Privacy  
 12 Expectations 68  
 13 Session 3: Big Data and Algorithms 136  
 14 Session 4: Economics of Privacy  
 15 and Security 188  
 16 Session 5: Security and Usability 250  
 17  
 18  
 19  
 20  
 21  
 22  
 23  
 24  
 25

4

1 alert building security.  
 2 We're almost done, just a few more items. The  
 3 building cafeteria is not open to the public today;  
 4 however, boxed lunches will be available for purchase in  
 5 the hallway outside of the auditorium and overflow  
 6 rooms. You may use the overflow rooms to eat lunch. No  
 7 food or drink, other than water, is allowed in the  
 8 auditorium.  
 9 The restrooms are in the hallway outside the  
 10 auditorium.  
 11 This is a public event, which is being webcast  
 12 and recorded. Welcome to everyone who is watching the  
 13 live webcast. An archived webcast and conference  
 14 materials will be available via FTC.gov after the  
 15 conference ends.  
 16 And, finally, we are live-tweeting today's  
 17 event under #PrivacyCon. Thank you, and over to Dan  
 18 Salsburg.  
 19 MR. SALSBERG: Thank you, Tina. I'm Dan  
 20 Salsburg, I'm the Acting Chief in the FTC's Office of  
 21 Technology, Research, and Investigation and a member of  
 22 the PrivacyCon team.  
 23 We know privacy and data security are  
 24 important to all of you gathered here today, and that  
 25 many of you are now seeing in person people who you knew

5

1 had preregistered for this event. We're sorry for  
 2 sharing that information with you last week, and are  
 3 addressing our bulk distribution setup to avoid such a  
 4 release from happening again.

5 I hope you have had a chance to review today's  
 6 agenda. We have a great and diverse roster of  
 7 presenters and participants and look forward to an  
 8 informative day of nonstop, cutting-edge presentations  
 9 covering the latest privacy and data security research.

10 Now, let's kick off PrivacyCon with remarks  
 11 from FTC Chairwoman Edith Ramirez, who has led the  
 12 agency's efforts to protect consumers from unfair and  
 13 deceptive privacy and data security practices.

14 Chairwoman Ramirez?  
 15 (Applause.)

16 CHAIRWOMAN RAMIREZ: Thank you, Dan. I'm  
 17 delighted to be here with you. So, good morning,  
 18 everybody, and welcome to PrivacyCon, a  
 19 first-of-its-kind conference at the Federal Trade  
 20 Commission bringing together leading experts to present  
 21 original research on privacy and data security.

22 Today, companies in almost every sector are  
 23 eager to scoop up the digital prints that we leave  
 24 behind when we post, shop, and browse online. The new  
 25 generation of products we see in the marketplace, from

6

1 smart appliances to connected medical devices to  
 2 semi-autonomous cars. All of these mean the consumers  
 3 must navigate an increasingly complex and dynamic  
 4 ecosystem. In short, the interplay between technology  
 5 and data is radically transforming how we interact with  
 6 everything around us. These trends will not only  
 7 continue, they will multiply.

8 At the FTC, we are constantly seeking to  
 9 expand our understanding of emerging technologies and  
 10 their impact on consumers as we work to ensure that  
 11 consumers enjoy the benefits of innovation, confident  
 12 that their personal information is being handled  
 13 responsibly. We know that enforcement and policy need  
 14 to be guided by research and data.

15 We do a great deal of research and analysis  
 16 internally, but with the increasingly rapid pace of  
 17 technological change and complexity of the privacy  
 18 challenges consumers face, more than ever, we need to  
 19 tap into the expertise and insights of the research  
 20 community to help us fulfill our consumer protection  
 21 mandate. Today's conference provides a unique  
 22 opportunity to do just that.

23 With PrivacyCon, our aim is to bridge the gap  
 24 between the academic, tech, and policy worlds. Our  
 25 ambitious agenda is filled with cutting-edge and

7

1 provocative research. Some of the presentations will  
 2 lend support for current privacy and data security  
 3 policies; others may lead us to rethink our assumptions.  
 4 Either way, we hope to spur a richer dialogue about  
 5 privacy and data security. And we hope that this  
 6 dialogue will be a two-way street.

7 As we seek valuable input from the academic  
 8 and tech communities, we also aim to provide useful  
 9 feedback to researchers about the type of work that  
 10 would be most relevant to helping us and other  
 11 policymakers make informed policy decisions.

12 So, this morning, to set the stage for our  
 13 program and to highlight the importance of research at  
 14 the FTC, I would like to speak very briefly about the  
 15 way that we've incorporated privacy and data security  
 16 research into our enforcement and policy work. The FTC  
 17 was founded on the principle that strong research  
 18 informs strong policy. Today, the agency serves as a  
 19 research and policy hub on a wide array of front-line  
 20 consumer protection and competition issues. Among them,  
 21 privacy and data security.

22 As you know, we've hosted workshops and issued  
 23 reports on significant and cutting-edge issues such as  
 24 facial recognition, the Internet of Things, data  
 25 brokers, mobile device tracking, mobile security, and

8

1 mobile privacy disclosures.

2 Our workshops have brought together academics,  
 3 consumer advocates, industry, technologists, and other  
 4 key stakeholders to help inform policy discussions, and  
 5 our reports on emerging technologies provide concrete  
 6 guidance to businesses on how to protect consumers in  
 7 today's digital world.

8 Most recently, we held a workshop on  
 9 cross-device tracking. To evaluate the benefits and the  
 10 risks of cross-device tracking, we need to know what it  
 11 is and how it works. Our workshop included a session  
 12 where experts explained how tracking techniques function  
 13 and discussed whether technical measures such as hashing  
 14 might be used to protect consumers' privacy.

15 And just last week, we issued our Big Data  
 16 report, which outlined a number of suggestions for  
 17 businesses to help ensure that their use of big data  
 18 analytics produces benefits for consumers while avoiding  
 19 outcomes that may be exclusionary or discriminatory.

20 In this report, we highlight possible risks  
 21 that could result from inaccuracies or biases about  
 22 certain groups and data sets, including the risk that  
 23 certain consumers, especially low-income or underserved  
 24 consumers, might mistakenly be denied opportunities or  
 25 that big data analytics might reinforce existing

9	<p>1 socioeconomic disparities.</p> <p>2 On the enforcement front, the work of tech</p> <p>3 researchers has helped us identify deceptive or unfair</p> <p>4 practices of companies such as HTC, Snapchat, and</p> <p>5 Fandango.</p> <p>6 Last month, we announced an action against</p> <p>7 Oracle in which we alleged that the company's failure to</p> <p>8 disclose that older, insecure versions of Java would not</p> <p>9 be removed as part of the software update process. We</p> <p>10 alleged that that was a deceptive practice. Various</p> <p>11 researchers had pointed out problems with malware</p> <p>12 exploits for older versions of Java, which led to our</p> <p>13 investigation of the issue.</p> <p>14 The consent order that we entered into</p> <p>15 requires Oracle to make an effective tool for</p> <p>16 uninstalling older versions of Java available to</p> <p>17 consumers. In short, our enforcement actions have</p> <p>18 provided important protections for consumers, and</p> <p>19 researchers have often played a critical role in helping</p> <p>20 us achieve that goal.</p> <p>21 In certain areas, we have also asked</p> <p>22 technologists and researchers to help us come up with</p> <p>23 technological countermeasures to address vexing</p> <p>24 problems. Illegal robocalls are a key example. Voice</p> <p>25 Over IP technology allows callers to spoof identifying</p>	11
10	<p>1 information such as the calling party's phone number.</p> <p>2 Fraudsters can now place millions of cheap, automated</p> <p>3 calls with the click of a mouse, and they can do so from</p> <p>4 anywhere in the world that has an Internet connection</p> <p>5 while hiding their identities in the process.</p> <p>6 These developments have reduced the</p> <p>7 effectiveness of the FTC's traditional law enforcement</p> <p>8 tools. Recognizing the need to develop new solutions,</p> <p>9 the FTC has held four public contests to spur the</p> <p>10 creation of technological solutions to the robocall</p> <p>11 problem. As part of these robocall challenges, we</p> <p>12 solicited technical experts to help select the most</p> <p>13 innovative submissions.</p> <p>14 One of the winning solutions in our first</p> <p>15 challenge, Nomorobo is in the marketplace and available</p> <p>16 to consumers. Nomorobo reports that it has more than</p> <p>17 360,000 subscribers and that it has blocked more than 60</p> <p>18 million robocalls.</p> <p>19 Given the importance of research and technical</p> <p>20 expertise in so much of the FTC's work, we are also</p> <p>21 continuing to build our internal capacity. Last year,</p> <p>22 we created the Office of Technology, Research, and</p> <p>23 Investigation, or OTech, as we call it. OTech, which</p> <p>24 builds on the work of our former mobile technology unit,</p> <p>25 identifies and conducts research that can guide the</p>	12
9	<p>1 development of enforcement and policy priorities, among</p> <p>2 other important work. The office's interdisciplinary</p> <p>3 team includes lawyers and technologists who work hand in</p> <p>4 hand to help us study new technologies and developments</p> <p>5 in the marketplace. With OTech, we're embarking on an</p> <p>6 even broader array of investigative research on</p> <p>7 technology-related issues that will aid us in all facets</p> <p>8 of the FTC's dual consumer protection and competition</p> <p>9 mission.</p> <p>10 PrivacyCon builds on all of these efforts.</p> <p>11 Our aim is to deepen our ties to the academic and tech</p> <p>12 communities and ensure that the FTC and other</p> <p>13 policymakers have the benefit of the leading thinking in</p> <p>14 the privacy and data security arenas.</p> <p>15 Our program today will feature five main</p> <p>16 topics. As to each, we'll have three or four short</p> <p>17 research presentations, followed by a period of</p> <p>18 discussion featuring top experts. We'll start with</p> <p>19 sessions addressing the current state of online privacy</p> <p>20 and consumer expectations about privacy. There's no</p> <p>21 question that, among other issues, we need to better</p> <p>22 understand consumer expectations and the degree to which</p> <p>23 consumer perceptions of companies' data practices align</p> <p>24 with what is actually happening in the marketplace.</p> <p>25 Just this morning, the Pew Research Center</p>	11
10	<p>1 released a study finding that Americans see privacy</p> <p>2 issues in commercial settings as contingent and</p> <p>3 context-dependent. In certain circumstances, a majority</p> <p>4 of Americans are willing to share their information if</p> <p>5 they perceive that they're getting value in return, and</p> <p>6 that their information is being protected.</p> <p>7 For instance, nearly half of those surveyed</p> <p>8 said that the basic bargain offered by retail loyalty</p> <p>9 cards is acceptable to them, while a third viewed that</p> <p>10 as unacceptable. But, while many consumers may be</p> <p>11 willing to share personal information in exchange for</p> <p>12 tangible benefits, the study also found that consumers</p> <p>13 are often cautious about disclosing their information,</p> <p>14 and frequently unhappy about what happens to that</p> <p>15 information once companies have collected it.</p> <p>16 We'll see what our speakers have to say about</p> <p>17 this and other topics. Our other sessions will address</p> <p>18 big data and algorithms, the economics of privacy and</p> <p>19 data security, and security and usability. Among the</p> <p>20 issues that will be addressed will be big data and bias,</p> <p>21 the economic incentives underlying companies' data</p> <p>22 practices, the cost of cyber incidents, and available</p> <p>23 options for consumers to avoid unwanted tracking.</p> <p>24 You will also hear from my colleague,</p> <p>25 Commissioner Julie Brill, and from our new Chief</p>	12

<p style="text-align: right;">13</p> <p>1 Technologist, Lorrie Cranor. And this is just to give 2 you a flavor of what you will hear today. 3 We are just now scratching the surface of what 4 is to come as a result of technological advancement. If 5 we want to ensure continued progress, we must craft 6 policies that are built on innovative thinking and 7 breakthroughs we make through research. And at the same 8 time, we want to encourage research that will aid the 9 complex and practical questions that policymakers are 10 eagerly seeking to answer. 11 So, thank you for being here today. Your 12 presence moves us one step closer to that goal. 13 Now, to close, let me just take this 14 opportunity to express my gratitude to all of the 15 participants in today's conference. We have an 16 incredibly impressive group of the top thinkers in 17 privacy and data security. I would also like to thank 18 the organizers in OTech and our privacy division, DPIP, 19 and in particular, Kristen Anderson and Dan Salsburg for 20 their hard work in putting this event together. So, 21 thank you very much. 22 (Applause.) 23 24 25</p>	<p style="text-align: right;">15</p> <p>1 they're over, you will know they're over, they will know 2 that you know they're over, so we will try to stay on 3 schedule. 4 After that there will be a short discussion 5 period. My co-discussants are Omer Tene from IAPP and 6 Elana Zeide from NYU, we will give a few thoughts, ask a 7 few questions and then that will be it. This is our 8 first time doing this, we would love your feedback, if 9 we're able to do this in the future and you apparently 10 have a lot of interest and that's great. 11 So, let me start out, I'm going to introduce 12 Ibrahim Altaweel from Berkeley to present on Web Privacy 13 Census 3.0. 14 MR. ALTAWHEEL: Hello, everyone. My name is 15 Ibrahim Altaweel, I am the co-author of Privacy Census. 16 Most people may believe that online activities 17 are tracked more pervasively now than they were in the 18 past. As early as 1999, Beth Givens of the Privacy 19 Rights Clearinghouse suggested that Federal agencies 20 create benchmark for online privacy. The census is one 21 such benchmark, and I'll discuss today how the 22 literature shows a dramatic upswing in the use of 23 cookies. 24 The first attempts at web measurement showed 25 relatively little tracking online in 1997. Only 23 of</p>
<p style="text-align: right;">14</p> <p>1 SESSION 1 2 THE CURRENT STATE OF PRIVACY 3 MR. BROOKMAN: Good morning, everyone. Thank 4 you very much, Chairwoman Ramirez. Thank you all for 5 coming out to our first PrivacyCon. I am Justin 6 Brookman, I am a policy director of the Office of 7 Technology Research and Investigation. We are 8 co-presenting this workshop along with the Division of 9 Privacy and Identity Protection. And I'm also the chair 10 of our first panel, The Current State of Online Privacy. 11 If my co-panelists could make their way to the 12 stage. 13 So, we put out our call for research 14 proposals, we weren't really sure what to expect. We 15 got nearly 90 really fascinating proposals, so 16 originally we were going to just try to do 12 or so, 17 which was tight. But we tried to pack the schedule so 18 we could have at least 19 people presenting, and we 19 honestly wish we could have done more. So, we have 20 tried to maximize the schedule to let them present their 21 research to you. They're each going to present for 22 about 15 minutes. We are going to try to keep them 23 aggressively to that. They have a clock right there 24 where it shows they're over time. They have a chime 25 that plays they're over time. So, they will know</p>	<p style="text-align: right;">16</p> <p>1 the most popular websites used cookies on their home 2 pages. But within a few years, tracking for commercial 3 advertising appeared on many websites. By 2011, all of 4 the most popular websites employed cookies. 5 In 2011, we started surveying the online 6 mechanisms used to track people online. We called this 7 our Web Privacy Census. We repeated that study in 2012 8 and in 2015. The main goal of the census is to collect 9 and analyze key metrics and measures, and monitor the 10 state of online privacy and use the results to answer 11 the following questions: How many entities are tracking 12 users online; what technologies are most popular for 13 tracking users; is there a shift from one tracking 14 technology to another in tracking practices; is there a 15 greater concentration of tracking companies online; what 16 entities have the greatest potential for online tracking 17 and why? 18 I will delve into some detail on the data 19 collection methods. We collected HTTP cookies, HTML5 20 local storage objects, and Flash cookies on the 21 Quantcast top 100, top 1,000 and top 25,000 websites 22 using OpenWPA, a web privacy measurement platform 23 developed by Princeton University. 24 We ran a shallow crawl and deep crawl. A 25 shallow crawl means that we only visited the home page</p>

17

1 of the popular websites, and a deep crawl means that we  
 2 visited the home pages and two links on the same  
 3 websites.  
 4 Data collection methods, of course, have some  
 5 limitations. For example, we used to have a Firefox  
 6 browser, so we don't have information regarding  
 7 different browsers. Another example is the crawler did  
 8 not log into any websites, which could potentially  
 9 result in more cookies being set. Overall, these  
 10 limitations mean that web privacy census is a  
 11 conservative measure of the amount of tracking online.  
 12 So, how much tracking is going on? We found  
 13 that users who merely visited the home pages of the top  
 14 100 most popular websites would collect over 6,000 HTTP  
 15 cookies, twice as many as detected in 2012. Some  
 16 popular websites use a lot of cookies. In just visiting  
 17 the home pages of popular websites, we found that 24  
 18 websites placed over 100 cookies, six websites that  
 19 placed over 200 cookies, and three websites placed over  
 20 300 cookies.  
 21 What technologies are most popular for  
 22 tracking users? One obvious observation is that there  
 23 are significantly more HTML5 local storage objects than  
 24 Flash cookies. HTML5 local storage is a new technology  
 25 that became popular in recent years for its large

18

1 storage capabilities, roughly a thousand times of Flash  
 2 cookies.  
 3 An increase in HTML5 does not directly  
 4 correlate with an increase in tracking, as an HTML5  
 5 storage object can hold any information that the browser  
 6 needs it to store locally. However, this information  
 7 can potentially contain information used to track users  
 8 and it can persist.  
 9 Is there a shift from one tracking technology  
 10 to another in tracking practices? We show the percent  
 11 from Flash cookies to HTML5 local storage, it is very  
 12 interesting to see that the total count of cookies has  
 13 increased, and there are more and more third party  
 14 cookies being used. 83 percent of HTTP cookies are set  
 15 by third-party hosts, and in just visiting the home  
 16 pages of popular websites, users would have cookies  
 17 collected by -- I mean cookies placed by 275 third-party  
 18 hosts. If the user browsed to just two more links, the  
 19 number of HTTP cookies would double.  
 20 Is there greater concentration of tracking  
 21 companies online? Google's presence on the top 100  
 22 websites increased from 74 in 2012 to 92 in 2015. The  
 23 percentage of cookies set by a third-party host has  
 24 increased from 84.7 percent to 93.5 percent.  
 25 So, what entities have the greatest potential

19

1 for online tracking and why? The most prominent one is  
 2 Google. We found that Google's tracking infrastructure  
 3 is number 92 of the top 100 most popular websites. And  
 4 on 923 of the top 1,000 websites, providing Google with  
 5 a significant surveillance infrastructure online.  
 6 Google's ability of tracking is unparalleled.  
 7 Most of third-party cookies are set by Google analytics  
 8 and Doubleclick. Facebook had a presence on 57 of the  
 9 top 100 websites and 548 of the top 1,000 websites. This  
 10 is important, because companies like Google can track  
 11 users almost as much as an Internet service provider  
 12 such as Verizon or Comcast.  
 13 In conclusion, the Web Privacy Census is a  
 14 modest research project that seeks to introduce reliable  
 15 empirical data on the issue of how much tracking there  
 16 is on the web. We have found, over a series of surveys,  
 17 covering three years, that there is a consistent upward  
 18 trend in cookie usage and that a small group of  
 19 companies have been tracking cookies almost everywhere  
 20 on the web.  
 21 In the future, we will continue to collect and  
 22 analyze key metrics and measures to monitor the state of  
 23 online privacy. Thank you very much. And I also would  
 24 like to thank my co-author, Nathan Good. Thank you.  
 25 (Applause.)

20

1 MR. BROOKMAN: Now we're going to hear from  
 2 Steven Englehardt of Princeton University on The Web  
 3 Never Forgets.  
 4 MR. ENGLEHARDT: Hello, everyone. I'm Steven  
 5 Englehardt from Princeton University, and today I'm  
 6 going to be talking to you about how the web privacy  
 7 problem is a transparency problem and show you the work  
 8 that we're doing to improve that.  
 9 So, when you're browsing the web, and you  
 10 visit a site, like let's say the New York Times, you're  
 11 not just visiting that first-party site, right, but  
 12 you're visiting all of the included third parties on  
 13 that site. And this might be people you recognize, like  
 14 Facebook provides social buttons or YouTube provides  
 15 video, but what about the advertising companies and the  
 16 analytics companies and so on that are not immediately  
 17 obvious who they are to the consumer?  
 18 Well, they could be, you know, anyone from  
 19 this graph, right? It could be, you know, users might  
 20 be able to figure out who they are if they use an  
 21 extension like Ghostery, but what are their privacy  
 22 practices, what are their tracking practices, which  
 23 technologies do they use?  
 24 That's not really obvious, right, because the  
 25 web lacks transparency, but what I'm going to show you

21	<p>1 today is how we're changing that. And I'll show you, 2 also, how we already have.</p> <p>3 So, throughout this talk, I'm going to talk 4 about and reference back to our paper from 2014, called 5 The Web Never Forgets. It's a paper that looked at 6 persistent tracking mechanisms, but in particular, I'll 7 focus on canvas fingerprinting. If you're not familiar 8 with canvas fingerprinting or that type of tracking 9 mechanism, essentially instead of setting some state 10 into the browser or instead of setting cookies on the 11 browser, you can look at the browser's properties and 12 use that to uniquely identify someone across different 13 websites, if you're a tracker.</p> <p>14 So, in 2012, there was a paper called Pixel 15 Perfect, which talked about canvas fingerprinting. Some 16 time over the next two years, AddThis, Ligatus and a 17 bunch of other companies, about 20 of them, starting 18 using this to track users.</p> <p>19 In 2014, we went and did our own measurement 20 of this. We wanted to see who was doing it, where they 21 were doing it, how the technology worked, and so on. And 22 then, shortly after releasing our paper, we saw a bunch 23 of news coverage, and this really surprised us. We 24 didn't expect such a response from the news and such a 25 response from users. Things like ProPublica, BBC and so</p>	23
22	<p>1 on.</p> <p>2 And then, just two days after all of that news 3 coverage happened, AddThis, who was the largest 4 provider, they provided canvas fingerprinting on 95 5 percent of their sites, they ended up -- they stopped 6 doing it. As well as Ligatus, which was the second 7 largest provider.</p> <p>8 So, the thing to point out here is that canvas 9 fingerprinting was a known technique for two years, but 10 in just two months following our measurement work, 11 people stopped using it.</p> <p>12 So, why was that? You know, what was 13 different about our work than just, say, having canvas 14 fingerprinting being known and having people know what 15 it was. And the key point is that our work removed the 16 information asymmetry between trackers and really the 17 rest of the web.</p> <p>18 So, like I said, we got a bunch of news 19 coverage from that, from different companies. And then 20 we saw users take to Twitter to complain about it, as 21 you can imagine. We saw people say, hey, you should 22 remove AddThis from your site, this is a way of 23 stalking, this is -- you know, the first parties here 24 are violating my privacy.</p> <p>25 We saw people -- we saw people just</p>	24
21	<p>1 complaining about it, and then we also saw someone say, 2 you know, I feel gross because I had to use AddThis to 3 show this, but everyone should know about canvas 4 fingerprinting.</p> <p>5 So, there was definitely a big response on 6 Twitter. And it wasn't just on Twitter, we also saw 7 people, for example, complaining to Mozilla and saying, 8 why doesn't Firefox protect me from this technique?</p> <p>9 And we even saw that it was beyond just users. 10 It was also between trackers and the sites that they 11 track on. So, ProPublica focused on YouPorn, which, of 12 course, they wanted to point out that this tracking is 13 happening there. And YouPorn responded to them and 14 said, hey, we didn't know AddThis was doing this, could 15 you -- you know, could you let your readers know, I 16 guess that we've removed AddThis from our site.</p> <p>17 So, we see that transparency is effective at 18 returning control to the users and the publishers of 19 knowing what's going on. The users can see what kind of 20 tracking technology is being used on their site and then 21 they can make decisions, right? They can complain -- or 22 you can see what kind of tracking technologies are on 23 the site that they visit, and then they can complain to 24 the first party or to the site that they're visiting. 25 They can choose not to go there, right? They can have</p>	23

25	<p>1 the communication between the browser and the sites that 2 we're visiting.</p> <p>3 And then we also have a Firefox extension 4 based off of Fourth Party. So, if you're not familiar 5 with that, it's another web measurement framework, 6 probably the most well used, prior to us building our 7 infrastructure, and we took all the features that that 8 had, added some more to it and built it right into our 9 platform as well.</p> <p>10 So, we give our researcher access to these 11 different locations in the browser and then we wrap that 12 up in something called a browser instance. And as you 13 can see here, we're basically able to run multiple 14 instances of Firefox or multiple browser instances at 15 the same time.</p> <p>16 So, when we do our own crawls, we run it over, 17 say, 20 browsers, and each one has their own 18 instrumentation. So, you can easily scale this up to do 19 measurement on a lot of sites.</p> <p>20 And there's a couple of things this lets us 21 do, right? We can keep a profile consistent through 22 crashes or freezes, so we can keep the same cookies as 23 we browse through different sites, just like a real user 24 would. We can also do things like run this with 25 extensions or privacy features, see how well they work.</p>	27	<p>1 I said before, is just a site goes and draws text to the 2 HTML5 canvas, and that text looks different on different 3 machines, but the same on the same machine. So, it's 4 useful if you want to differentiate between different 5 users but keep -- you know, know who the same user is.</p> <p>6 As you can see here, the differences can be 7 quite large. This is just a visualization of the 8 differences between different machines compared to each 9 other.</p> <p>10 And I want to give credit to all the 11 co-authors of this study. I was just one part of it. 12 So, we worked with people at KU Leuven and a bunch of 13 other co-authors at Princeton.</p> <p>14 So, the way that this works is a website will 15 draw a bunch of canvas -- a bunch of text to the canvas 16 and make it overlapping and try to maximize the chance 17 that it's unique and that's what you see visualized up 18 here. And if we want to measure this, we have to do a 19 few things. We first had to write a Firefox patch to 20 look for when these methods were called, when right text 21 or when pulling back the canvas has a string when that 22 happens.</p> <p>23 We had to write -- sorry, we had to write 24 automation with Selenium to go and run this across a 25 bunch of sites, and build that from the ground up. And</p>
26	<p>1 See if they're actually protecting users or where 2 they're falling short. And if there's any new web 3 technologies being used for tracking, like WebRTC or 4 audio and so on, we can take a look at that.</p> <p>5 So, this is already used by seven research 6 groups, and you just heard a great presentation by the 7 Web Privacy Census guys who do it, but it's also used 8 beyond academia from journalists and regulators.</p> <p>9 So, I'll talk a little bit about the 10 measurements we're doing. We're going on monthly crawls 11 of a million sites and we're collecting things like all 12 the JavaScript calls that might be used for 13 fingerprinting, or all the JavaScript files on all of 14 those sites so we can go and check out what's actually 15 going on later on. And we're also looking at, you know, 16 the requests and responses, and different storage 17 locations in the browser.</p> <p>18 And this lets us do a bunch of things, like 19 see how effective privacy tools are, like Ghostery or 20 Adblock Plus, see how effective browser protections are, 21 see how JavaScript might be used for tracking, and also 22 look at tracking practices.</p> <p>23 So, now I'm going to give you two quick case 24 studies. I'll go through canvas before we built 25 OpenWPM, I'll go through WebRTC after. So, canvas, like</p>	28	<p>1 then, of course, we had to write some analysis code on 2 top of that.</p> <p>3 And now I'm going to show you how things were 4 easier to measure another technique that could 5 potentially be helpful for tracking. If you're not 6 familiar with WebRTC, it's a -- or WebRTC for using it 7 for local IP discovery, essentially it adds some 8 networking capabilities into the browser that you can 9 access from JavaScript. And basically, you're able to 10 get the user's local IP, if they're behind in that. If 11 you're a home user, that might be something like 12 192.168.1.2, but it can be useful for tracking. You can 13 think of it like that.</p> <p>14 So, I saw a tweet that this was happening and 15 I said, oh, we can measure that, you know, we can take a 16 look at that, this won't be that hard. So, I was able 17 to add just a single line of JavaScript into our next 18 crawl to do this. So, this is the same thing I -- you 19 know, I have a method here that allows you to look at 20 any time anyone accesses WebRTC and I can see that, 21 right? I can see what they're setting and what they're 22 doing with it.</p> <p>23 And it's the same method I use to look at 24 who's doing things with canvas, right? So, it's just 25 one added line of code to run our crawls.</p>

29	<p>1 I had to write some analysis code on top of 2 that, very similar to canvas, right? With canvas. I 3 want to know who wrote text and who read back from it. 4 Well, here I do similar things to see when this 5 technique is being used. 6 And I found this happening on a bunch of 7 sites, beyond the New York Times, right? The New York 8 Times actually stopped doing it. So, 121 first-party 9 sites, and 24 of those were unique, only one of which is 10 blocked by, say, Adblock Plus or other similar privacy 11 tools. So, if you're going to be using privacy tools, 12 this technique may still be able to run on your machine. 13 And I guess the point I want to make here is 14 that web measurement gets much easier with OpenWPM. 15 Instead of writing a Firefox patch, we could just write 16 a single line of JavaScript. And instead of writing 17 automation with Selenium, we could just use OpenWPM. 18 And, of course, we still need to write the analysis 19 code. You always need -- you always need some extra 20 human component in there, but the first two steps got a 21 lot easier. 22 So, where do we want to go with it? We think 23 we can use this to inform the public, right? Let people 24 know, hey, here's what's happening on the sites you're 25 visiting. Here's who's doing canvas fingerprinting, and</p>	31	<p>1 And then, lastly, in the future, we hope that 2 you will be able to download our data and build some 3 analysis of your own on top of it. We will be, you 4 know, going further with that in the coming months. 5 So, if you want to help us make the web more 6 transparent, you can check out our GitHub repo to 7 collaborate, or you can check out our research page. 8 Thank you. 9 (Applause.) 10 MR. BROOKMAN: Thank you very much, Steven. 11 Now we're going to hear from Chris Hoofnagle 12 with a critique of Alan Westin's Homo Economicus. 13 MR. HOOFNAGLE: Good morning, everyone. I 14 wanted to start by thanking the Federal Trade Commission 15 and, in particular, its staff for putting together this 16 event. The different researchers presenting today are 17 very substantive and I am proud to be among them. I 18 think you have done a fantastic job, and thank you, you 19 should be proud. 20 My team at Berkeley over the years has shown 21 different ways that websites and other web services 22 track people. For instance, my team published the first 23 big paper about Flash cookies, explaining how Flash 24 cookies could be used to override users' cookie 25 deletion, and we also showed how HTML5 paired with</p>
30	<p>1 we think that will really help people understand what's 2 going on when they're browsing the web. 3 We want to provide data for privacy tools. 4 Disconnect, which is a privacy tool, like Adblock Plus 5 or like Ghostery, they actually ended up taking the 6 scripts that we released as part of our canvas study and 7 building it into their own tool, so they protected 8 against canvas fingerprinting. 9 We want to provide that same kind of data for 10 other privacy tools with our future studies. And we 11 also want to make the data accessible to less technical 12 investigators who may want to dig through it themselves, 13 but maybe don't have all the skills necessary to dig 14 through it at the same level that, say, someone who 15 writes the code would do. 16 And we would also love to collaborate with 17 people. So, you can -- you know, the infrastructure is 18 open source, you can go and GitHub, and I'll have a link 19 on the next slide to use it. You can download it, and 20 if you see anything wrong with it or if you see needed 21 features, you are welcome to submit back to it. 22 We also envision people using it to run their 23 own measurements like the Web Privacy Census. That's an 24 awesome use case and we really hope that more people 25 start doing that.</p>	32	<p>1 JavaScript could be used to do very similar things. 2 And the theme of that work was a conflict 3 between the kind of rhetoric one hears here in 4 Washington about users being in control and users being 5 able to make choices about how they are tracked online 6 and the technical reality. The technical reality that 7 even mainstream companies could use Flash and JavaScript 8 to override deleted cookies. It was an attack that 9 looked somewhat like a computer crime. 10 My presentation today is in a similar vein. 11 It's about the conflict between theory and rhetoric, and 12 how consumers actually operate in the marketplace. The 13 FTC's notice and choice approach to consumer information 14 and privacy is based on the idea that consumers follow a 15 rational choice model of making decisions online. 16 Now, the problem with notice and choice then 17 becomes that the model of a homo economicus, the model 18 of the rational consumer who is making choices in the 19 marketplace has to be reliable as a model. So, much of 20 my talk today is about the tradeoff talk. The idea that 21 people are making tradeoffs in the marketplace on 22 privacy. 23 The theoretical background, of course, is 24 about rational choice theory, and I am going to skip 25 over a bunch of slides to stay on time today, but the</p>

<p style="text-align: right;">33</p> <p>1 key point of my paper is that Alan Westin's theory was  2 based in rational choice theory, and his main thesis was  3 that public policy should serve the privacy pragmatists,  4 so these are the people who weigh choices in the  5 marketplace and make decisions according to their  6 privacy preferences.  7 So, we're familiar with these different  8 definitions, the privacy fundamentalists, the  9 pragmatists and the unconcerned, but let me draw your  10 attention to some of the verbs Westin used to describe  11 the privacy pragmatists. If you look at the verbs,  12 they're all highlighted in bold here. These are all  13 active characteristics of consumers. The privacy  14 pragmatists are people who weigh evidence. They are  15 people who examine evidence. They look to see whether  16 fair information practices are being widely observed.  17 This is an active, engaged consumer. I,  18 frankly, don't know many people who are like this. I'm  19 not even sure that I'm like this. But this is the basis  20 for much of U.S. policy on consumer decisionmaking and  21 privacy. And, of course, Westin famously said, in the  22 politics of privacy, the battle is for the hearts and  23 minds of the privacy pragmatists. These are the people  24 we should be paying attention to and these are the  25 people who policy should be designed for.</p>	<p style="text-align: right;">35</p> <p>1 consumers simply won't answer one of the questions. So,  2 I'll show you in our studies, we found that somewhere  3 between two and almost five percent of consumers  4 wouldn't answer one of the three questions. What do you  5 do with people who don't answer the questions? In  6 Westin's methods, you make them privacy pragmatists.  7 That's really problematic.  8 And it explains, another critique we have in  9 the paper, that Westin never academically published his  10 work. In part because I don't think it was publishable.  11 This work, excuse me, this work I don't think was  12 publishable.  13 So, moving on, another way to look at the data  14 is empirically, and this is where I'm standing on the  15 shoulders of people such as Professor Turow. Turow  16 pointed out years ago that when you ask people about the  17 rules of privacy, most of them don't get the basic  18 answers right. He shows essentially that consumers  19 think that the privacy policy is a seal. Most consumers  20 think, for instance, that if a privacy policy is merely  21 present, that website cannot sell personal information  22 to third parties.  23 And it's for this reason that we should be  24 very skeptical of tradeoff talk. People don't  25 understand the tradeoff to begin with, and I'm going to</p>
<p style="text-align: right;">34</p> <p>1 Well, how did Westin come to the segmentation  2 of Americans? The way he did it was by asking this set  3 of questions. One had to deal with consumer control;  4 one had to do with whether data were treated  5 confidentially; and, finally, the last question is kind  6 of an attitudinal question about whether law and  7 self-regulation is sufficient for privacy.  8 So, my first critique focuses on this  9 segmentation text. On the most basic level, the problem  10 with Westin is that he segmented -- he segmented it such  11 so people were pragmatists by default, and this  12 semantically doesn't make sense, because we're not  13 pragmatists by default. Pragmatism requires affirmative  14 action. It requires a certain outlook on life. And I  15 would argue that pragmatism is actually quite  16 controversial. There are many Americans who find  17 pragmatism quite distasteful, but yet he coded it as the  18 default result.  19 There are some other problems here. Westin's  20 questions, the screening questions used, really had  21 nothing to do with pragmatism. There's nothing in there  22 asking, you know, do you read privacy policies, how much  23 time do you spend researching products and the like?  24 It's just not in there.  25 And then, finally, a significant number of</p>	<p style="text-align: right;">36</p> <p>1 get to a second reason of why we should be skeptical of  2 it.  3 Turow, of course, was standing on the  4 shoulders of other people in the privacy field,  5 including Oscar Gandy, in his initial view of Westin's  6 data, he viewed knowledge of privacy as a powerful  7 explanatory factor of why people care about privacy in  8 how they make decisions.  9 So, this is where a lot of my work picked up,  10 and I wrote a number of studies with fun -- well,  11 actually, the fun covers started when I stopped writing  12 with Joe, the Joe covers are boring, but my covers, I  13 think, are more exciting. You'll see the Parthenon  14 marbles in all my studies because I think they're quite  15 beautiful.  16 You know, what we did, and starting in looking  17 at Californians, what we did is we asked people about  18 their privacy knowledge, and we found a funny thing. The  19 privacy fundamentalists were always more correct than  20 the other groups about existing law and traditional  21 practices. And not only that, people who shopped online  22 were less knowledgeable of rules and practices than  23 people who didn't shop online. Strange. Right? You  24 would think those people shopping online would read the  25 privacy policy.</p>

37

1 So, we did a whole bunch of surveys over the  
2 years where we presented people with quizzes asking them  
3 questions that Turow used, and that other investigators  
4 used, and we found over and over that the basics, people  
5 failed on the basic quizzes. Just as an example, in our  
6 2009 survey, 75 percent answered two or fewer questions  
7 correctly, 30 percent got none of them correctly, and  
8 then people say, well, the digital natives are going to  
9 save us. This is a generational problem. The digital  
10 natives are going to figure this out.

11 No. They are actually the worst performers in  
12 the group. Both online and off, when we asked about  
13 offline privacy.

14 So, we replicate the study again in 2012, and  
15 we find, again, that there's a -- that there are  
16 substantial misconceptions about people's rights and  
17 about what practices are, and we find over and over  
18 again, and the three stars mean a P value of 0.001, that  
19 the privacy fundamentalists are more knowledgeable than  
20 other groups, the other groups that are so-called, who  
21 apparently don't care, or who are making tradeoffs.

22 So, the main point of our paper is that  
23 Westin's segmentation has confused pragmatism with  
24 ordinary consumer decisionmaking, and that most -- many  
25 consumers in the marketplace are something uninformed.

38

1 They're viewing privacy policies essentially.

2 Another major part of this paper is the idea  
3 about whether people -- whether Americans are more  
4 concerned about government collection of personal  
5 information or private sector personal information  
6 collection, and what we found over and over in our  
7 surveys is that Americans are concerned about both.

8 And this is not just our findings. If you  
9 look at the major literature reviews in Public Opinion  
10 Quarterly, and these are the -- you know, these are the  
11 political scientists who study privacy and they write  
12 these amazing literature reviews looking at all of the  
13 different studies over decades. They find, going back  
14 to the 1980s, Americans say they're just as concerned  
15 about the private sector as they are with the government  
16 sector.

17 So, we argue, basically, that RCT as a model  
18 fails in this field because people are laboring with  
19 substantial misconceptions about their rights. And they  
20 do care about those rights.

21 Let me say something, finally, about Westin.  
22 Westin was a fantastic academic, and his work, his  
23 academic work, was great. He is truly a generator of  
24 American information on privacy. In his book, Privacy  
25 and Freedom, as you probably have heard, Omer's group

39

1 has republished it and it's worth a read.

2 Alan Westin was against technology  
3 determinism, which is a philosophy one hears a lot of in  
4 D.C., and he also saw privacy as a liberal value. So,  
5 his survey work I critique today is not his academic  
6 work, and I have a lot of respect for that academic  
7 work.

8 So, what do we do? What are the implications  
9 for FTC practice? Among them, we can start viewing  
10 privacy policies as seals. When you go to the  
11 marketplace and you buy the organic vegetable, you don't  
12 look for an organic policy. You look for -- you assume  
13 that organic means certain things. We could start  
14 saying that privacy means certain things.

15 Now, the FTC has already started to do this in  
16 security. If your privacy policy says anything about  
17 security, it requires some type of reasonable control  
18 over personal information.

19 Another approach comes from the history of the  
20 Federal Trade Commission. In the 1970s, the Federal  
21 Trade Commission started recruiting marketing academics  
22 to come in-house at the PCP, and this greatly punched up  
23 the Federal Trade Commission's understanding of how  
24 consumers were misled by false advertising. And if you  
25 look at today's Commission actions, their false

40

1 advertising theories are much more in line with how  
2 consumers really understand ads, how consumers really  
3 act, and that has not come over to the privacy side.

4 So, we could replicate that. And then,  
5 finally, I do think that we need to look at unfairness  
6 more as a remedy for privacy problems. Now, why is  
7 this? Notice and choice might work in a world where  
8 you're selling physical products, but we are not doing  
9 that in this world. These are personal information  
10 products, and the transactions are not discrete, the  
11 transactions are continuous.

12 That means that lock-in, shifting practices,  
13 network effects, are all ways in which companies can  
14 shape choices and in effect remove choice from the  
15 consumer. And I write about this in much greater detail  
16 in this paper with Jan Whittington.

17 Finally, let me just say thank you, and I  
18 can't avoid making a pitch for my book, which discusses  
19 these issues in much greater detail. And I do know that  
20 the ad practices division is not in attendance today, so  
21 what I'll say about that is, if you read this book  
22 instead of eating chocolate and other things, you are  
23 guaranteed to lose weight, without exercise.

24 (Laughter.)

25 (Applause.)

41	<p>1 MR. BROOKMAN: Thanks, Chris. And, finally, 2 we are going to hear from Professor Joe Turow from the 3 University of Pennsylvania on The Tradeoff Fallacy. 4 MR. TUROW: Hello. Thank you. I am going to 5 go through this fairly quickly. It's a lot of stuff to 6 talk about, but I wanted you to get a sense of the arc. 7 The idea here, a summary, is that marketers justify 8 their data collection with the notions that Americans 9 want and understand the benefits of data tradeoffs. We 10 challenge this assertion with the results of a national 11 telephone survey. Further, we present evidence that 12 what observers interpret as tradeoff behavior is really 13 widespread resignation among Americans regarding 14 marketers' use of their data. So, that's the point. 15 It's not what we sometimes interpret as tradeoffs and 16 can be looked at when people do things as, gee, they're 17 doing tradeoffs, is really reflective of resignation of 18 a large proportion of the population. 19 Okay, so what's the issue? Polls repeatedly 20 find that consumers are concerned about ways marketers 21 access and use their data online. And there are studies 22 from Annenberg, from Pew, from Bain &amp; Company, 23 reflecting that. At the same time, observers agree that 24 people often release data about themselves that suggests 25 much less concern about that, okay? That's called by</p>	43	<p>1 mean by it. 2 Generally, though, firms argue that consumers' 3 understanding of tradeoffs along with increasing 4 consumer power justifies consumer data collection and 5 use. The big deal today is that consumers have this 6 huge power with the use of the mobile phone, the use of 7 the Internet and other ways, and as a result, companies 8 have to push back sometimes in order to maintain some 9 kind of profitable relationship. 10 And marketers increasingly see personalization 11 resulting from predictive analytics as a savior in an 12 age of hyper-competition. So, this is a great quote 13 from Yahoo. "This concept of value exchange for 14 personal data is starting to come to life through 15 personalization, that it's a pathway to advertising 16 nirvana." 17 Now, the tradeoff justifies 360-degree 18 tracking. We can go into a whole lot of detail about 19 this stuff. I just wanted to cite Gartner, a consulting 20 firm. They talk about four stages through what they 21 call cognizant computing that will unroll over the next 22 two to five years, it was written I think two years ago, 23 with the first two well under way. They call them "sync 24 me, see me, know me, be me." And it's the idea of 25 really getting to know people as much as you can</p>
42	<p>1 many people the privacy paradox. The notion that people 2 say they love privacy, but in everyday life, it's 3 different. They don't. They give it up. They give up 4 data for anything. 5 Some marketers read this paradox as evidence 6 that people place other things above privacy, which 7 leads to the notion of tradeoffs that Chris was talking 8 about. For example, Yahoo says that online Americans 9 "demonstrate a willingness to share information as more 10 consumers begin to recognize the value and the benefit 11 of allowing advertisers to use data in the right way." 12 And the president of Mobiquity says, "The average person 13 is more than willing to share their information with 14 companies if these organizations see the overall gain 15 for end-users as a goal, not just for themselves." This 16 reflects some of the rational choice thinking that Chris 17 was alluding to. 18 A few corporate voices in papers, white papers 19 by Accenture, Bain, Brand Bond Loyalty, have put 20 cautions around such generalization. For example, Bain 21 says customers' trust can't be bought by companies 22 offering compensation in exchange for selling or sharing 23 personal data. And others have urged transparency, but 24 really not saying what transparency means. They use the 25 word, but it's very difficult to figure out what they</p>	44	<p>1 data-wise in almost an organic way to figure out what's 2 going on and how to make money off of them. 3 All right, but there are alternative 4 explanations to tradeoffs. One is the public's lack of 5 knowledge of what marketers are doing with their data 6 behind the computer screen. Chris talked about some of 7 that. A lot of surveys show that lack of knowledge. And 8 Cranor and McDonald, Lorrie and Aleecia, found that 9 people really don't understand privacy policies. 10 Alessandro Acquisti and others talk about the 11 difficulty of understanding the technological and 12 institutional systems. Essentially, this knowledge 13 failure research explains the ease with which data 14 retailers and advertisers retrieve information from 15 individuals. So, the proposition hasn't been directly 16 tested, but it might get marketers off the hook too 17 easily, so we say, gee, people have a lack of knowledge. 18 It's because the schools don't teach them enough. Or 19 let's figure out an educational program. 20 Ad choices, those little icons that you are 21 supposed to see, I gave a talk at the Penn law school 22 one day showing a slide and nobody saw it, okay? And, 23 but, they can point to this to sound more optimistic 24 about what the public is than people like me or 25 policymakers about this.</p>

45	<p>1 So, we did a survey to try to look at some</p> <p>2 hypotheses related to this. A 20-minute, on average,</p> <p>3 interview taking place in February/March 2015,</p> <p>4 English-speaking or Spanish-speaking, 750 landline,</p> <p>5 wireless 756, conducted by Princeton Survey Research</p> <p>6 Associates. More data about that is in the paper.</p> <p>7 We looked first at people's philosophy of</p> <p>8 tradeoffs, not the particulars, but what do they know</p> <p>9 about, what do they think about the idea of tradeoffs?</p> <p>10 And you can see it says, if companies give you a</p> <p>11 discount, it's a fair exchange for them to collect</p> <p>12 information about me without my knowing it; 91 percent</p> <p>13 said no. Is it fair for an online or physical store to</p> <p>14 monitor what I'm doing online when I'm there in exchange</p> <p>15 for letting me use the store's wireless Internet or WiFi</p> <p>16 without charge; 71 percent said no. Is it okay if a</p> <p>17 store where I shop uses information it has about me to</p> <p>18 create a picture of me that improves the services they</p> <p>19 provide about me; 55 percent said no.</p> <p>20 Now, oddly, if we look at all of how many</p> <p>21 people agreed with all three propositions, only four</p> <p>22 percent agreed with all three propositions. We took a</p> <p>23 broader idea of what agreement was when we gave numbers</p> <p>24 to each, like agree strongly, agree, disagree, disagree</p> <p>25 strongly, and in that broader interpretation of belief</p>	47	<p>1 may make. So, for example, you might say I'll take the</p> <p>2 discount, but what if you know what the supermarket is</p> <p>3 doing with your data? This is knowledge Americans</p> <p>4 almost never receive directly, but may intuit from ads</p> <p>5 and coupons they think are targeted toward them.</p> <p>6 So, we have a variety of things we asked them</p> <p>7 that said, will you accept it, to the people who said</p> <p>8 they would accept the discount in the first place, we</p> <p>9 said, would you accept it if they -- accept it if the</p> <p>10 supermarket makes assumptions based on your purchases</p> <p>11 about whether you buy low-fat foods, it went down to 33</p> <p>12 percent. The more we asked particular questions about</p> <p>13 individuals' lives, the less they said they would do it.</p> <p>14 So, in the end, when we asked about social/</p> <p>15 ethnic background inferences, only 19 percent said they</p> <p>16 would accept it.</p> <p>17 The table shows the limits of cost-benefit</p> <p>18 analyses as a rationale for marketers' claims that most</p> <p>19 people will provide personal data in exchange for store</p> <p>20 deals. The decline in acceptance from 43 percent to</p> <p>21 around 20 percent isn't consistent with marketers'</p> <p>22 assertions that people are giving up their personal</p> <p>23 information because of cost-benefit analysis.</p> <p>24 In the supermarket scenario, they're doing</p> <p>25 just the opposite, resisting the idea of giving data for</p>
46	<p>1 in tradeoffs, we found there's still a small proportion,</p> <p>2 21 percent believes that common tradeoffs with marketers</p> <p>3 amount to a fair deal.</p> <p>4 But we wanted to look at the privacy policy in</p> <p>5 terms of a scenario of real life. So, we said, for the</p> <p>6 next few questions, please think about the supermarket</p> <p>7 you go to most often. Let's say this supermarket says</p> <p>8 it will give you discounts in exchange for its</p> <p>9 collecting information about all your grocery purchases.</p> <p>10 Would you accept the offer or not? Fifty-two percent</p> <p>11 said no, 43 percent said yes, which is interesting,</p> <p>12 because it's closer to that other of the three</p> <p>13 statements we said it's okay if a store where I shop</p> <p>14 uses information it has about me to create a picture,</p> <p>15 you say, well, that's those 43 percent. It turns out</p> <p>16 it's not, because when we looked at it, we found that</p> <p>17 only 40 percent of the people who accept that dictum</p> <p>18 agreed with the supermarket thing.</p> <p>19 Those people are very inconsistent. The lack</p> <p>20 of correspondence, even when the scenarios appear</p> <p>21 similar, underscores that a small percentage</p> <p>22 consistently accepts the idea of tradeoff.</p> <p>23 We wanted to know whether people who say they</p> <p>24 will accept the supermarket discount will still do it</p> <p>25 when presented with specific assumptions a supermarket</p>	48	<p>1 discounts based on some kind of analysis. Then we went</p> <p>2 ahead and our hypothesis about resignation came out of</p> <p>3 our everyday realization when we met people, they would</p> <p>4 say things like, gee, you know, I have to give up the</p> <p>5 data, I have to be online, I have to be on Facebook, I</p> <p>6 know they do this stuff or I don't know what's going on,</p> <p>7 but I have to do it anyway.</p> <p>8 So, we gave the people two statements</p> <p>9 separated by many other statements so they weren't right</p> <p>10 next to each other, I want to have control over what</p> <p>11 marketers can learn about me, I've come to accept that I</p> <p>12 have little control over what marketers can learn about</p> <p>13 me. Okay? It turns out that 58 percent of people agree</p> <p>14 with both statements, which we say indicates a sense of</p> <p>15 resignation. Resignation meaning the acceptance of</p> <p>16 something undesirable but inevitable. I got that from</p> <p>17 Google, Google Dictionary.</p> <p>18 We found there's a strong positive statistical</p> <p>19 relationship between believing in tradeoffs and</p> <p>20 accepting or rejecting various kinds of supermarkets'</p> <p>21 use of discounts. You would expect that. By contrast,</p> <p>22 there's no statistical relationship between being</p> <p>23 resigned to marketers' use of data and accepting or</p> <p>24 rejecting the supermarket tradeoff. People who are</p> <p>25 resigned, sometimes they do, sometimes they don't. They</p>

1 try and navigate a world that they don't understand, are  
 2 annoyed about, possibly, and they sometimes will do it.  
 3 They may look like they're accepting tradeoffs, but in  
 4 their heads, they're saying, gee, I'm resigned to it.  
 5 Put another way, people who believe in  
 6 tradeoffs give up their data predictably, while people  
 7 who are resigned don't do it in a predictable manner.  
 8 They do give up their data, though. We found 57 percent  
 9 of those who took the supermarket deal were resigned. A  
 10 much smaller 32 percent were tradeoff supporters, even  
 11 using the broader measure of tradeoff support that I  
 12 suggested.  
 13 The larger percentage of people in the  
 14 population who are resigned compared to those who  
 15 believe in tradeoffs indicate that in the real world,  
 16 people who exchange their data for benefits are more  
 17 likely to do it while resigned rather than as a result  
 18 of cost-benefit analysis.  
 19 Moreover, we found that resignation is  
 20 widespread across the U.S. population, regardless of  
 21 age, gender, education or race. There were no  
 22 statistical differences between age and gender, there  
 23 were between education and race, but still, the large  
 24 percentage of people were resigned anyway.  
 25 We found that most Americans don't have basic

1 population that is resigned about a key aspect of its  
 2 everyday environment.  
 3 Now, this may sound really dark, and, you  
 4 know, what do you do about it, but I think it's really  
 5 important to confront what I see in everyday life when I  
 6 talk to people, that people do these things online, in  
 7 stores, with apps, not because they're thinking in a  
 8 cost-benefit way rationally, but because they feel that  
 9 they have no other choice if they want to live in this  
 10 world.  
 11 We're only at the beginning of key aspects of  
 12 this era. This is the beginning of a new era, not even  
 13 the middle. And there may be time for concerned parties  
 14 to guide it. Academics, journalists, and advocates have  
 15 to translate the key issues for the public, and there  
 16 are a lot of issues of obfuscation and deception that we  
 17 can talk about. Issues that the FCC might be involved  
 18 in around public interest, convenience and necessity.  
 19 The importance that people have alluded to in praising  
 20 and naming groups that do right things and not so right  
 21 things.  
 22 Thanks for listening.  
 23 (Applause.)  
 24 MR. BROOKMAN: Thank you, Joe. Thanks to all  
 25 of our presenters, and now we're going to move into a

1 knowledge to make informed cost benefit choices. This  
 2 is some of the stuff that Chris was talking about, 51  
 3 percent can't recognize the possibility of phishing.  
 4 Large percentages believe incorrectly that government  
 5 and laws protect them from price discrimination and  
 6 certain forms of data collection, when they don't.  
 7 These widespread misconceptions suggest that  
 8 even when Americans do weigh the costs and benefits of  
 9 giving up their data, they frequently base those choices  
 10 on incorrect information. But we also found, and this  
 11 really was surprising to me, that those who know more  
 12 about marketing laws and practices are more likely to be  
 13 resigned. We found, too, that resigned people who  
 14 accept supermarket discounts, even as the supermarket  
 15 collects increasingly personal data, have more knowledge  
 16 than others.  
 17 So, having more knowledge is not protective as  
 18 future -- as a protective feature as some academics have  
 19 suggested.  
 20 So, what do we do about it? The rationale of  
 21 tradeoffs is a fig leaf, we argue, used by marketers to  
 22 justify a world of tracking and increasingly  
 23 personalized profiling that people know is there, don't  
 24 understand, and say they don't want. We haven't begun  
 25 to consider the social implications of having a large

1 brief period of discussion. There's one caveat, Joe may  
 2 have to leave early, he's teaching two classes later  
 3 today at Penn, so if you see him slink off, he's not in  
 4 trouble, we are not angry with him, he's not mad at us.  
 5 So, I'm go to start with some of the trends I  
 6 saw from the presentations. There's one, the  
 7 proliferation and growing sophistication and growing  
 8 complexity of online tracking is reflected in Abe's and  
 9 Steven's work. There are more cookies, there are more  
 10 companies who are doing it. I love the revised  
 11 Lunascape chart, with all the hundreds of thousands of  
 12 companies that you couldn't even see them on this big  
 13 screen. And more technologies, too, right? It's not  
 14 just cookies, it's HTML5, it's fingerprinting, it's  
 15 ETags, it's audio beacons, it's endless.  
 16 And then logically, perhaps unsurprisingly,  
 17 the theory of Joe and Chris' argument is that there's an  
 18 increasing inability of consumers to really manage or  
 19 control their privacy, given all these advances. So,  
 20 the idea that a consumer goes to a website and reviews  
 21 the privacy policy and makes an informed choice that I  
 22 am satisfied with how ETags are used on the site and I  
 23 will now access my content in exchange for that is  
 24 flawed.  
 25 And this builds somewhat on Lorrie Cranor's

<p style="text-align: right;">53</p> <p>1 work that if you had to read every single privacy 2 policy, it would take like months of your life. And, 3 so, instead of that, it sounds like that there's this 4 resignation, right? Instead of privacy pragmatism, 5 there is resignation. This is what Joe's work was 6 talking about. 7 This hit home with me this weekend, I went 8 skiing with a friend of mine and we were talking and he 9 said he sent a link to his dad to a news story and his 10 dad called him and said, "I'm not opening that, do you 11 know how many cookies are in there?" And he was like, 12 yeah, I know. I mean, he's not a privacy guy, neither 13 of them, and he's like, yeah, I know, but what are you 14 going to do, right? You could have tried to walk 15 through deleting cookies or installing Adblock, but he 16 had to pick up his kids, right, he didn't have time to 17 really think about everything in his question. And 18 we've all talked to people who have had similar 19 experiences, we have all probably had similar 20 experiences ourselves. I don't really know what's going 21 on here, but I just don't have the time to figure it 22 out. 23 And it's not just the web, right, I mean, it's 24 the Internet of Things, we had our cross-device tracking 25 workshop, we're letting TVs or toasters collect</p>	<p style="text-align: right;">55</p> <p>1 importantly, the sort of experts, advocates, 2 policymakers, academics. And with that seems to also be 3 a shift from the idea of questioning consumers' 4 decision-making capabilities to whether they're, in 5 fact, actually engaging in a choice at all, or you're 6 resigned because they see no agency and no reasonable 7 alternatives to opting out of the mainstream, or because 8 they have trusted the default system. 9 If you look at the idea of what transparency 10 is as a means to solve those issues and accomplish that, 11 I think there are several implications based on this 12 research. One is how do you use transparency as a way 13 to galvanize consumers to articulate their preferences 14 or to engage in privacy self management, if, in fact, it 15 may lead to their being more resigned because they have 16 a feeling of helplessness? 17 Also, how do you ensure or predict when 18 companies will actually be prompted by public opinion to 19 make a change, and whether those changes will actually 20 occur without regulation or other enforcement mechanisms 21 for the most meaningful private potential privacy 22 abuses, and which might also be most likely to be the 23 most profit-generating core of many companies' 24 businesses. 25 There's also the question of whether</p>
<p style="text-align: right;">54</p> <p>1 information about us. It's physical space with 2 automatic license plate readers, and are we making an 3 informed choice when we go outside with facial 4 recognition. 5 And, so, one thing I would like to hear from 6 the folks about, and I am going to turn it over to my 7 other co-discussants first, is, so what does the 8 solution look like, right? I mean, do we just ride it 9 out? There are a lot of folks who say that Brandeis was 10 concerned about cameras, and we're cool with cameras 11 now. Do we want government making, you know, rules 12 about how much tracking can happen if consumers can't 13 make the choices themselves? Say 15 cookies and that's 14 it. 15 And, so, the point of PrivacyCon is we can 16 hear from really smart people who are thinking about 17 this to help them influence, you know, policy decisions. 18 And, so, I would love to hear some of their thoughts or 19 solutions later. 20 And I will ask you a question about that, but 21 first I'm going to turn it over to Elana. 22 MS. ZEIDE: So, one interesting theme I'm 23 noticing is a shift away from the idea about informed 24 notice for individuals but more transparency for the 25 collective populus, including both consumers and, more</p>	<p style="text-align: right;">56</p> <p>1 transparency can operate as a mechanism to ensure 2 consumer trust in a world where there are unknowable 3 unknowns. Years ago, people would allow their friends 4 to post pictures on Facebook without thinking that their 5 picture would remain in obscurity because they weren't 6 being tagged. In an age of facial recognition, that is 7 no longer true. I think these shifts really undermine 8 consumers' sense of what they can predict and how their 9 choices -- a sense of helplessness in the sense of the 10 unknown and what may happen in the future. 11 Finally, I am interested in the idea of 12 whether a move towards transparency or shaming and 13 blaming creates a system where we may be able to get 14 some clarity about consumer norms and what standards 15 infer. It may also create a situation where 16 sensationalist media stories or small vocal subsets who 17 resist certain practices end up controlling the 18 conversation and give a false sense of clear consensus. 19 And the last point would be, does this then 20 entail a system where we must wait for harms and abuses 21 to occur before we can then create systems to correct 22 them, and if so, does that imply that along with some 23 transparency mechanisms we also need mechanisms that 24 consumers can see for due process and redress? 25 MR. BROOKMAN: All right.</p>

57

1 MR. TENE: Thank you. So, I think all four  
2 presentations here drew sort of a grim and somber  
3 picture of the state of play today with consumers being  
4 misled or resigned and kind of being dragged along for  
5 the ride by technology or by business. Given that the  
6 stars seem aligned like this, I feel an urge to play  
7 devil's advocate, and in that role, I am going to  
8 suggest a couple of different adjectives to describe how  
9 consumers are acting or feeling or faring.

10 Instead of being resigned, I'll suggest that  
11 they're actually thrilled or maybe even exhilarated or  
12 delirious about these new technologies, about the fact  
13 that, you know, they can hail an Uber and rate the  
14 driver, and get like the newest iPhone or Android phone,  
15 and, you know, even, yippy, take like a selfie and post  
16 it on their Snapchat story, or use a Fitbit and sort of  
17 give up their fitness or health information. And I  
18 think we clearly see that in the marketplace.

19 We also see Google and Facebook and Apple as  
20 three of the -- Microsoft, three or four of the  
21 strongest brands in terms of brand recognition in the  
22 market, and not to mention the number of people flocking  
23 to work in these places, including people who are now in  
24 government and even regulatory agencies.

25 So, the point is that there seems to be

58

1 something more complex at play here, and, you know, I  
2 think we see it in other contexts. So, I care about  
3 health, but I still eat a cheeseburger. I care about  
4 the environment but I drive a four-wheel drive. There's  
5 a lot of snow in New England. And I think part of your  
6 response, your report will be yes, but consumers are  
7 ignorant, they just don't know, but actually, I think  
8 Joe's survey and research shows that the more informed,  
9 they actually become more resigned. So, maybe it's  
10 better to just be blissfully ignorant.

11 So, with all that, I want to turn back to you  
12 and hear a reaction.

13 MR. TUROW: I mean, these are really important  
14 insights. I think that it's a complicated world. It's  
15 very hard not to be excited about the ability to walk  
16 through a store and compare prices in your hand. There  
17 are levels of excitement about being able to show a kid  
18 a snippet from The Wizard of Oz on a phone on a bus when  
19 the kid is starting to get antsy. I mean, there are lot  
20 is of things that are terrific about this.

21 I couldn't live without Google. But what I'm  
22 saying, where I'm coming from, anyway, is that I think  
23 part of my job is to say -- I mean, there are a lot of  
24 companies who are saying all these great things, but  
25 underlying it, there are some real problems that we have

59

1 to face.

2 And I think part of being a citizen in this  
3 society is to say, yeah, there are terrific things about  
4 this, but there are also things that in the long term  
5 might -- and I really do believe this -- might harm our  
6 democracy. Might harm our relationship with others.

7 When you walk through a store now, and you're  
8 not sure what profile the store has about you, when not  
9 too long from now you can get on your phone, and in some  
10 places it already exists, different prices based upon  
11 who you are. That's a scary thing to me in terms of how  
12 are people going to understand the public's fear, their  
13 relations to others? How are people going to understand  
14 the political process when they think they're getting  
15 information that is developed personally for them that  
16 are personal ads?

17 So, while I agree that there are many terrific  
18 things about this, I think that there have to be  
19 segments of society that have to say, stop, we can fix  
20 the really difficult things that relate.

21 MR. HOOFNAGLE: But let me unravel some of the  
22 issues that -- and there are -- what I'd say is that,  
23 first, that one can look at our work and say it's  
24 anti-technology, but I would argue strongly that it is  
25 not, and I personally love technology and I'm an early

60

1 adopter of many, many things.

2 I'm also a practitioner, and I do know that  
3 much of what we call innovation does not depend on  
4 personal information, and is fundamentally compatible  
5 with what Alan Westin would call modern information  
6 privacy law, such as we're going to de-identify this  
7 information after six months, we're going to delete it  
8 after a year, et cetera.

9 So, I think the -- one of the rhetorical --  
10 it's in the way a strawman that we have to recognize and  
11 deal with, is the idea that we can't have privacy and  
12 these technologies. We can have Uber. Uber is actually  
13 not that innovative. You know, long before Uber, taxi  
14 cab companies had hail apps in mobile. You don't need  
15 personal information for a lot of that.

16 But when you do need personal information, you  
17 have rules around it. And I see it from practice all  
18 the time. There are situations where we do very  
19 interesting forms of personalization, with de-identified  
20 data, where we agree that data will disappear after a  
21 certain amount of time, where we agree that certain  
22 things won't be the basis of selection and the like.

23 So, I think we shouldn't fall into the false  
24 dilemma that privacy means we cannot have a spectacular  
25 convenience in our life.

61

1 MR. ENGLEHARDT: So, coming at this from I  
2 guess the tracking perspective, I wanted to comment on  
3 the fear of, you know, maybe users becoming resigned by  
4 getting more information about what tracking was going  
5 on, or the notion that we can't have the services  
6 without having the tracking.

7 Because I think there is definitely a chance  
8 that if everyone starts fingerprinting and users just  
9 see, oh, every site I'm visiting is fingerprinting me, I  
10 guess I just have to deal with it. Like that could  
11 happen, but I think we could prevent that from happening  
12 with the right policies and with the right tools where  
13 consumers could protect themselves by releasing that  
14 data for not just the consumers, but for everyone.

15 And then, the notion that consumers might, you  
16 know, see -- or consumers just have to be tracked. I  
17 don't think that's really true either, because a lot of,  
18 at least for advertisers that support opt-outs, right,  
19 you should be able to set up an opt-out cookie and not  
20 be tracked, but we still see that fingerprinting often  
21 goes on when those opt-out cookies are set.

22 So, perhaps there should be some enforcement  
23 that if you're going to tell users you've opted out of  
24 tracking, you can also guarantee you won't do things  
25 like fingerprinting, and the user doesn't just have to

62

1 trust that that won't happen. So, thanks.

2 MR. BROOKMAN: I'll ask one more question.  
3 And if we come to the broader policy question of what's  
4 the alternative, because I've talked to a lot of  
5 companies, and they kind of tell the same story, right?  
6 Oh, of course consumers can't control all this stuff,  
7 but they argue that really means there should be more of  
8 an accountability model, right? Companies should be  
9 responsible stewards of the data, right? Consumers can  
10 be in control, the company should make smart, informed  
11 decisions about how the information is used.

12 Because what is the alternative to that?  
13 That's one option, right? And then there is the FTC or  
14 the government could be making prescriptive policy  
15 choices on behalf of people. You know, that has its  
16 problems as well. One threat we've heard a few times  
17 today is the idea of increased transparency and then  
18 filtered through elites or institutions, and the  
19 name-and-shame approach that Joe and Steven talked  
20 about, and Elana talked about in her comments.

21 And I guess my question is, is that scalable,  
22 right? I mean, you know, Wall Street Journal did their  
23 What They Know series starting in 2010, and yet the  
24 reports you guys show is that the tracking that they  
25 were concerned about is still increasing. Joe and Chris

63

1 have been doing this for even longer.

2 You know, so what is the policy solution,  
3 assuming that, you know, there is a problem to be  
4 addressed, you know, what is the right approach?

5 MR. TENE: Can I jump in and say that --

6 MR. BROOKMAN: Yes.

7 MR. TENE: Thank you. That I think, you know,  
8 and also reacting to what Chris and Joe said, I think  
9 there is consensus that we need to deal with data  
10 excess, and have, like, de-identification, and clearly  
11 we need strong data security, but I think to a large  
12 extent, industry gets it. And certainly industry gets  
13 the big impact that privacy fails can have on brand and  
14 consumer expectations, and I think one thing that  
15 attests to this is the fact that we are having this  
16 conference and the existence of the privacy profession  
17 that has blossomed so the IPP now has 25,000 members  
18 worldwide that had less than 10,000 just two and a half  
19 years ago.

20 I think the right processes are in place, and  
21 it's really the excess that we need to deal with. And I  
22 think you illustrated some of this in the technological  
23 research.

24 MR. HOOFNAGLE: Well, the access and  
25 accountability issues have to be dealt with, and there

64

1 were very interesting proposals to focus mainly on use  
2 of data, but I think one weakness of those proposals is  
3 they don't take into account the attacks on  
4 accountability that are occurring, such as the Spokeo  
5 case. You know, if you take the Spokeo case seriously,  
6 and if you read the Amici briefs, a large portion of the  
7 technology industry is arguing that they should be able  
8 to willfully violate the law. Willfully. That means  
9 they know what the law is and they violate it anyway.  
10 And that they shouldn't be able to be sued.

11 Wyndham was, in a way, an attack on  
12 accountability. You know, the class action, we don't  
13 like class actions. We don't like the FTC doing  
14 anything. We don't want Congress to do anything. So,  
15 where exactly does the accountability come from?

16 And I think when you look at use models, the  
17 first defense, the first time someone gets caught in a  
18 use violation, they're going to make an IMS Health  
19 argument. And, so, I think if we're going to move  
20 toward a use model, the accountability is going to have  
21 to include a contractual waiver of First Amendment  
22 defenses, and an agreement that there is injury in fact  
23 that supports standing. Otherwise you will never be  
24 able to sue. Not even you, Justin. If you take the  
25 position seriously, not even the FTC would be able to

65	<p>1 sue.</p> <p>2 MR. TENE: I think, you know, some companies</p> <p>3 have staked radical positions and, frankly, I think done</p> <p>4 themselves a disservice, which is something that I think</p> <p>5 is prone to occur in litigation. On the whole, you</p> <p>6 know, the FTC has been successful, and I'm not sure how</p> <p>7 much traction the First Amendment argument against</p> <p>8 privacy accountability will have. We'll see.</p> <p>9 MS. ZEIDE: So, one question I have following</p> <p>10 up on that is, so, when you talk about use and the</p> <p>11 assumption of harm, are you looking at -- it seems like</p> <p>12 use is almost in this case a broader word to really talk</p> <p>13 about data-driven decision-making. And is that, I</p> <p>14 think, where you see the troubles lie?</p> <p>15 MR. HOOFNAGLE: I would like to defer to</p> <p>16 someone else, because it is not my area of expertise.</p> <p>17 MR. ENGLEHARDT: So, can you repeat that</p> <p>18 question?</p> <p>19 MS. ZEIDE: So, I'm just saying, in this case,</p> <p>20 when we talk about what the abuses are and the sort of</p> <p>21 harm, is it really about the uses in terms of the</p> <p>22 tracking and what people are theoretically doing with</p> <p>23 information, or abstractly, or does it really become an</p> <p>24 issue when there's data-driven decision-making?</p> <p>25 MR. ENGLEHARDT: So, I think -- I guess the</p>	67	<p>1 should be worried about how it could be abused down the</p> <p>2 road?</p> <p>3 MR. HOOFNAGLE: I've written pretty</p> <p>4 extensively about the need to focus on collection</p> <p>5 because of the inability to police uses, and I think to</p> <p>6 get to a point where we can police use, we need to</p> <p>7 really see change and a form of accountability that</p> <p>8 doesn't really exist.</p> <p>9 What my team has found over and over, when we</p> <p>10 discover things like HTML5 or Flash cookie responding,</p> <p>11 we go to the companies and we say, we think you're doing</p> <p>12 this, and they say, no, we're not doing it. And they</p> <p>13 actually don't know that they're doing it.</p> <p>14 MR. BROOKMAN: Any other closing thoughts?</p> <p>15 (No response.)</p> <p>16 MR. BROOKMAN: And with that, we are over</p> <p>17 time. Thank you all so much. We are going to have a</p> <p>18 quick 10-minute break and then we will come back with</p> <p>19 our next session.</p> <p>20 (Applause.)</p> <p>21 (Whereupon, there was a recess in the</p> <p>22 proceedings.)</p> <p>23</p> <p>24</p> <p>25</p>
66	<p>1 fear, like I would say it's more of the data use, right?</p> <p>2 It's the fear that if this data is being collected, how</p> <p>3 is it being used? And that the consumer has no ability</p> <p>4 to go and prevent that collection or no ability to</p> <p>5 control that collection beyond, like, preventing it from</p> <p>6 happening, right? So, once the data gets put into the</p> <p>7 company's databases, that kind of is up to trust.</p> <p>8 MR. BROOKMAN: I mean, so I guess it kind of</p> <p>9 goes to the point, I mean, so should we be concerned</p> <p>10 about the collection itself, right? You guys both had</p> <p>11 in your studies, like, there's a lot more collection</p> <p>12 going on. And, like, I'm sure there a lot of people in</p> <p>13 the room are like, yeah, but it's not bad collection,</p> <p>14 right? It's not malicious collection. It's being done</p> <p>15 to support the ad ecosystem, which there's nothing</p> <p>16 inherently wrong with that, and then there has</p> <p>17 definitely been folks who have said that FTC should be</p> <p>18 focused on the cases where there is the harm down the</p> <p>19 road, right?</p> <p>20 Commissioner Ohlhausen has written about this,</p> <p>21 there has been a lot of focus on the use of data for</p> <p>22 discrimination, right? We have a panel on that later</p> <p>23 today. I mean, so should we be focused at the FTC or</p> <p>24 policy in general be concerned about the raw collection</p> <p>25 in the first place, or is it just the fact that we</p>	68	<p>1 SESSION 2</p> <p>2 CONSUMERS' PRIVACY EXPECTATIONS</p> <p>3 MS. ANDERSON: Please take your seats. We're</p> <p>4 about to start with the next session. Good morning, I'm</p> <p>5 Kristen Anderson, and I'm an attorney with the Division</p> <p>6 of Privacy and Identity Protection within the FTC's</p> <p>7 Bureau of Consumer Protection. I'm here to do the</p> <p>8 second session of the day, which is on consumers'</p> <p>9 privacy expectations.</p> <p>10 We will hear from six researchers in four</p> <p>11 15-minute presentations, and then we will conclude with</p> <p>12 about 20 minutes of discussion where we will identify</p> <p>13 common themes and ask the presenters about their work</p> <p>14 and its implications.</p> <p>15 Without further ado, I will introduce our</p> <p>16 first presenter. We have Serge Egelman of the</p> <p>17 International Computer Science Institute at the</p> <p>18 University of California at Berkeley. Serge will start</p> <p>19 us off with his presentation on Android permissions.</p> <p>20 Serge?</p> <p>21 MR. EGELMAN: Thank you for that introduction.</p> <p>22 So, this is work that I have been doing with</p> <p>23 several students recently where we've been looking at</p> <p>24 privacy and how private information is regulated on</p> <p>25 mobile platforms. So, to give you I guess a brief</p>

69

1 overview, most of this work is on Android, and that's  
2 only because Android actually has a pretty intricate  
3 permission system to try and implement notice and  
4 choice.

5 So, whenever an application requests access to  
6 certain sensitive data, it's regulated by this  
7 permission system, and so when users install an  
8 application, they see a screen that informs them of all  
9 of the possible types of sensitive data that that  
10 application might be requesting in the future.

11 And, so, the question was, does this actually  
12 implement effective notice and choice? So, do users  
13 understand these messages about how applications could  
14 be using their data in the future?

15 So, we started this project a couple of years  
16 ago by doing an online survey. We had over 300 Android  
17 users, and we just showed them screen shots of these  
18 permission screens, and simply asked them if an  
19 application was granted these abilities, what might that  
20 allow the application to do.

21 We then followed that up with a qualitative  
22 study where we had 24 people come to our laboratory, and  
23 we interviewed them about similar concepts. And what we  
24 concluded from this was that many people were simply  
25 habituated, since these appear every time people install

70

1 applications, not only does it list what abilities and,  
2 you know, types of sensitive data that application is  
3 requesting in the future, but all the possible types  
4 that it could request, even if the application never  
5 takes advantage of that.

6 And, so, people become habituated. They see  
7 lots of these requests that have lots of different data  
8 types, some of which they don't understand, and  
9 therefore, they learn to ignore these, because there's  
10 just so much information there. Another problem was  
11 that people were simply unaware. Since this occurs  
12 whenever you install an application, a lot of people  
13 said that, oh, this is just part of the license  
14 agreement, and we know that we need to click through  
15 that in order to continue installing the application.  
16 So, maybe this occurs at the wrong time in the process.

17 And since it happens after the user clicks  
18 install, it could be that they are already committed to  
19 installing the application; there are various cognitive  
20 biases that relate to this, and so therefore it's  
21 unlikely that they are actually comparison shopping  
22 based on privacy, even if they wanted to.

23 Another issue is that understanding of whether  
24 a particular application is going to access a particular  
25 type of data really requires a good understanding of

71

1 this whole permission system, and what are the different  
2 types of data that are regulated by the permission  
3 systems.

4 So, you know, understanding whether an  
5 application is requesting a data type requires  
6 understanding the whole universe of data types that are  
7 governed here.

8 And, so, we made these recommendations, and  
9 what we concluded was that a lot of this could be taken  
10 away. So, transparency is great. Notice and choice is  
11 good, but the problem is, when people are overwhelmed by  
12 the notice, which is what we see with privacy policies  
13 on websites, they eventually just ignore it all, because  
14 there's so much information.

15 So, you know, what we found was that a  
16 majority of these permissions could probably just be  
17 granted automatically without showing the user lots of  
18 information, because either the dangers are very low  
19 risk. For instance, you know, changing the time, for  
20 instance, or causing the device to vibrate, or is simply  
21 reversible. So, you know, if an application does abuse  
22 one of these abilities, chances are the user can find  
23 out about it and simply undo it and there's no lasting  
24 harm in that.

25 At the same time, there are a few very

72

1 sensitive things, which because of doing this at install  
2 time, that's probably the wrong time during the process,  
3 the user has no context about how the data might be used  
4 in the future, these could probably be replaced with  
5 runtime dialogues. But another open question is, this  
6 is just looking at all of the different abilities and  
7 data types that could be requested by an application. We  
8 didn't look at how frequently these data types and  
9 abilities are actually used in reality.

10 And, so, things actually improved. So, we did  
11 this study two or three years ago in the most recent  
12 versions of both Android and iOS. They now have a few  
13 runtime dialogues that prompt the user at the time that  
14 an application is going to first request access to  
15 certain sensitive data types. But the problem with this  
16 is it also -- well, so it adds some contextual  
17 information. The user is doing something, this dialogue  
18 appears, and then they could probably use information  
19 about what they were doing to make a decision about  
20 whether this request is reasonable or not. So, maybe  
21 clicking a button to find things near you, it then would  
22 be expected that an application would request access to  
23 GPS data.

24 The problem with this is, it only appears the  
25 first time that data type is requested. Once this is

73

1 granted, the user never sees one of these dialogues  
2 again. And, so, future access to that type of data  
3 might be under completely different circumstances that  
4 might actually surprise the user or be really  
5 concerning.

6 And, so, another question we have is, how  
7 often are these types of data on mobile platforms really  
8 accessed in practice? And, so, we performed another  
9 study, last summer, where we looked at real applications  
10 in the wild, and we instrumented the Android operating  
11 system so that every time one of these data types is  
12 requested by a third-party application, we made a log of  
13 it. And then we gave these instrumented phones to 40  
14 people, 36 of them returned said phones, and then we  
15 ended up with a pretty robust data set.

16 So, each time one of these sensitive data  
17 types was requested, and I'm talking about things like  
18 access to the contact list, GPS data, things like that.  
19 We also requested -- we also collected things about what  
20 the user was actually doing on the phone. So,  
21 contextual data. Things like the time stamp, whether  
22 the application that was requesting this data was even  
23 visible to the user, so whether the application was  
24 running in the background, maybe the screen was off.  
25 Most people don't realize that, you know, applications

74

1 might not be visible to the user and are still  
2 accessing, you know, data on the phone.

3 Connectivity, location, what part of the  
4 application they are currently viewing. So, what UI  
5 elements were exposed, that might yield some information  
6 about whether or not this access to sensitive data was  
7 expected or not. And then also the history of other  
8 applications that were run.

9 So, we let people use these phones for about a  
10 week. We transferred their actual real data on them, so  
11 they were using them as they would their normal phones,  
12 they popped their SIM cards into them. And then  
13 afterwards, at the end of that week, they came back to  
14 our lab, and we gave them some questionnaires. We  
15 randomly showed them some screen shots that occurred  
16 during the course of that week and then asked them  
17 questions.

18 So, these screen shots were taken randomly  
19 whenever one of these sensitive data types was accessed,  
20 so that we can ask them, as a prompt, you were doing  
21 something, this is what you were viewing on the screen  
22 of your phone, it was requesting this particular type of  
23 data, how -- you know, was that expected? Did you  
24 expect that application to be requesting that particular  
25 data type at this moment in time? And also, if you were

75

1 given the ability to, would you have prevented that from  
2 happening?

3 And, so, we used that as ground truth to see  
4 whether we could actually predict whether a user would  
5 have wanted that data to be accessed by the application  
6 or not. And, so, this resulted in, you know, we had 36  
7 people participate, we had over 6,000 hours of real-time  
8 usage, and during that one-week period with 36 people,  
9 we found 27 million requests for sensitive data that was  
10 protected by this permission system.

11 So, some of the problems that we found were  
12 due to incorrect mental models. So, again, you know,  
13 the goal of this is transparency, show the user all the  
14 possible ways that an application might be accessing  
15 sensitive data. Is that really working?

16 Well, we found that in 75 percent of cases,  
17 the application that was requesting one of these data  
18 types was completely invisible to the user. So, this  
19 was mainly due to the screen being off, in 60 percent of  
20 the cases. So applications running, you know, the user  
21 wasn't actually using their phone. Or background  
22 services.

23 Another thing that we found was, despite the  
24 fact that there are some privacy indicators built into  
25 the operating system, so both Android and iOS have

76

1 indicators for when GPS is accessed. There's a -- this  
2 is an example of one of those indicators, it appears in  
3 the top status bar and most people assume that, you  
4 know, the only time that GPS information is collected,  
5 this icon will appear.

6 It turns out that's not true at all. And, in  
7 fact, the icon only appears in 0.04 percent of the cases  
8 where location data was accessed. And that's because  
9 every time an application requests location data, the  
10 operating system caches that for performance reasons and  
11 also to preserve battery life, but then when another  
12 application accesses just the cached location data as  
13 opposed to querying the GPS hardware directly, this icon  
14 never appears.

15 Similarly, applications can infer your  
16 location based on cellular network data, nearby WiFi  
17 hotspots, and it turns out most applications are using  
18 those methods to infer location, rather than the GPS  
19 hardware. And therefore, most of the time, when location  
20 data is collected, people have no indication that that's  
21 occurring.

22 So, you know, what if -- so, having this, the  
23 notice and choice at the beginning when users install  
24 the application obviously doesn't work. We've tested  
25 that. The ask on first use that's currently happening

77	<p>1 isn't really working because of the different contexts 2 in which users might be interacting with applications. 3 So, maybe we could have runtime requests all 4 the time, so every time applications request data, we 5 can have a little notice appear. Well, obviously that's 6 really impractical, too. So, you know, the 27 million 7 data points that we collected, that would result in, per 8 person, about 200 popups per hour, most of which is due 9 to requests for location data, but you could see that 10 there are other data types that were pretty frequently 11 requested. And, so, having lots of popups appear on the 12 phone is not really a good way of going forward either, 13 because that's also going to lead to habituation. 14 But at the same time, in our exit survey, what 15 we found was that the vast majority of participants said 16 that given the opportunity, they would have denied at 17 least one of these requests, and on average, you know, 18 they would have denied a third of the requests. 19 So, how do we do this? How do we give users 20 control over the things that they actually care about 21 without overwhelming them? So, we're doing some work 22 now to try and predict the cases where applications 23 access data where people would want to know that this is 24 occurring, whereas the other ones where applications 25 access data that might be expected, well, obviously we</p>	79	<p>1 But one of the main things we also observed 2 was that the data was really nuanced. So looking at one 3 user's preference and comparing that to another didn't 4 really work among our 36 participants, because there was 5 just so much variance in the data with regard to what 6 people wanted and what their expectations were. Which 7 suggests that, you know, having a one-size-fits-all 8 solution about what people care about and what should 9 they be shown is unlikely to work either. And, so, 10 maybe we need more intelligent systems that can predict 11 user preferences on a per-user basis. 12 So, going forward, we're actually trying to 13 implement these systems right now that can try and 14 predict a given user's preferences based on their 15 previous behaviors. And this is part of a pretty 16 complex ecosystem. So, we have what we're calling hard 17 policy, which is preferences that people have explicitly 18 stated. So, I don't want applications to be using data 19 for X reason, and then trying to augment that with soft 20 policy. So, inferred preferences that systems can make 21 about users, such as maybe looking at, you know, 22 hundreds of thousands or millions of users, we can infer 23 one user's preferences based on other users who are like 24 them. Like recommender systems. 25 And also, you know, based on the feedback from</p>
78	<p>1 shouldn't prompt the user in those cases. 2 And, so, what we found was that expectations 3 really did predict behavior in this case. So, we asked 4 people if this access to personal data was expected or 5 not, and then whether they would have blocked it, there 6 was a pretty strong correlation there. 7 We also found that using the current model on 8 ask on first use, so if you look at for each unique 9 application, in each unique data type, if you ask users 10 the first time that application requests that data, 11 we're going to get it right about 50 percent of the 12 time, which is what's currently happening. So, that's a 13 coin flip. 14 But we also found that looking at, you know, 15 the visibility of the application was a pretty strong 16 predictor of user expectation. So, applications running 17 in the background requesting data were pretty often -- 18 those were unexpected. And, so, if we add that to the 19 equation, we can get this right about 85 percent of the 20 time. So, instead of just asking on the first use, we 21 could ask the first time that the application requests 22 the data in the foreground and then ask the first time 23 the application requests the data in the background, and 24 then we're going to get it right about 85 percent of the 25 time.</p>	80	<p>1 prompts. So, if we can design more efficient prompts 2 that cater to individual user expectations, we can then 3 use the output of those, so what did the user actually 4 decide to ensure that they see fewer prompts in the 5 future. And that's it. I'll leave it at that. 6 So, well, the conclusion is, you know, notice 7 and choice is great, the problem is figuring out what 8 notice to give people, since attention is a finite 9 resource. So, I'll leave it at that. 10 (Applause.) 11 MS. ANDERSON: Thank you, Serge. 12 Next we will hear from Ashwini Rao of Carnegie 13 Mellon University about mismatched privacy expectations 14 online. 15 MS. RAO: Hello, thank you. So, yeah, my talk 16 is about expecting the unexpected, understanding 17 mismatched privacy expectations online. 18 So, I'll start with the motivation. So, many 19 of us on a daily basis interact with online websites, 20 and as we interact with online websites, we may have 21 questions, such as what types of data does this website 22 collect about me, how does it share this data, and does 23 it allow deletion of this data? 24 And to answer these questions, a user could 25 read the website's privacy policy, which is usually a</p>

<p style="text-align: right;">81</p> <p>1 textual document in English, and it discloses the data 2 practices of the website, such as collection, sharing, 3 and deletion; however, these policies in their current 4 form are long and difficult to read. So, users usually 5 ignore them. 6 So, the main motivation is, how can we help 7 users understand online data practices? And our 8 approach is to focus on user expectations. So, we 9 assume here that users expect websites to engage in 10 certain data practices. For example, users may expect 11 banking websites to collect financial information and 12 health websites to collect health information. 13 And these expectations may vary based on 14 context; for example the type of website or user 15 characteristics: Age, their privacy knowledge, their 16 privacy concern. However, user expectations may not 17 match what websites actually do. For example, users may 18 not expect banking websites to collect health 19 information. 20 Now, the question here is could we generate 21 effective privacy notices by extracting and highlighting 22 these data practices that do not match user 23 expectations? 24 So, the concept is simple. A privacy notice 25 does not have to inform you about things that you</p>	<p style="text-align: right;">83</p> <p>1 privacy research has predominantly not focused on 2 multiple types of expectations. 3 So, in our research, we make a distinction 4 between two types of expectations. The first: 5 Expectation in the likelihood sense. What does the user 6 expect that the website will do versus what does the 7 user expect the website should do? And this is in the 8 desired sense. And then we compared that with 9 practices, data practices of websites. 10 To measure expectations, we conducted user 11 studies. So, one of the user studies that we conducted 12 focused on the expectation in the likelihood sense. And 13 in future, we also plan to measure expectation in the 14 desired sense. So, we presented users with different 15 types of websites, and then after the users interacted 16 with these websites, we asked them, what do you assume 17 that the website will do? 18 And once we elicited user expectations, we 19 next extracted the data practices from privacy policies, 20 and then we compared these two to identify mismatches. 21 So, in our study, we used -- we varied the website 22 characteristics and user characteristics. So, as I 23 mentioned earlier, user expectations can vary based on 24 these website and user characteristics. 25 We looked at 17 different data practices,</p>
<p style="text-align: right;">82</p> <p>1 already expect or know. A privacy notice has to inform 2 you about things that you do not expect or do not know. 3 So, I want to make a distinction between 4 policy and notice. A policy is usually a textual 5 document, but a notice, which is based on the policy, is 6 usually more -- is usually shorter and more usable. 7 So, here I'm showing you the privacy nutrition 8 label, which focuses on visual format, and so far, 9 notices that make -- that are more effective, our 10 research has focused on visual formats. And our 11 approach of extracting and highlighting mismatched 12 expectations is complementary to this approach. 13 Once we identify and extract these mismatched 14 expectations, we could present them to the user in any 15 visual format that is effective. I also want to say 16 here that these privacy notices do not have to be 17 generated or provided by the website operators 18 themselves. These could be provided by a third party, 19 for example through a browser plugin. And this is 20 something important to note. 21 So, the main research questions are how do we 22 define expectation, and how do we measure expectations, 23 and identify mismatches in these expectations? So, 24 research in nonprivacy domains shows that users can have 25 different types or multiple types of expectations. And</p>	<p style="text-align: right;">84</p> <p>1 which were split among collection, sharing, and 2 deletion. And for collection and sharing, we looked at 3 four different types of data: Contact information, 4 financial, health, and current location information. 5 So, here's an example scenario. So, here the 6 scenario is describing the collection of different types 7 of data when the user does not have an account on the 8 website. So, you can see that we are asking the user, 9 what is the likelihood that this website will collect 10 your contact information? 11 So, in future if we wanted to also measure 12 desired expectations, we could also ask them, do you 13 think the website should be or should not be allowed to 14 collect this information, in addition to do you think 15 it's likely that the website would or would not collect 16 this information. 17 So, we deployed the study as an online survey, 18 and we studied in total 16 websites. We had 240 19 participants that we recruited from Mechanical Turk 20 crowdsourcing platform. 21 So, this was to elicit user expectations, the 22 latter part is to actually extract data practices from 23 privacy policies. And to do this, we used two 24 annotators, two experts, one in the privacy domain and 25 another in the legal domain, and they manually read</p>

85	<p>1 these policies and answered questions such as does this 2 policy disclose that the website collects health 3 information? 4 Now, to scale up, we are also developing 5 techniques that are semi-automated and that use natural 6 language processing and machine learning that can go and 7 extract answers to these questions. So, the annotations 8 say whether a website is clear, whether it engages in 9 the sort of practice, it does not engage; whether it's 10 unclear or the policy does not contain any statements 11 that addresses this data practice. 12 Now, it's important to note that there can be 13 different types of mismatches. Here I'm showing you 14 two, the yes/no mismatch and a no/yes mismatch. And 15 this is important because the type of mismatch can 16 impact users' privacy differently. 17 So, consider the yes/no mismatch. The website 18 states that, yes, we collect your information, but the 19 user thinks, no, the website is not collecting my 20 information. 21 So, in this case, the user may go ahead and 22 actually use the website, and unknowingly give up data. 23 And lose privacy. Whereas in the no/yes mismatch, the 24 website is saying, no, we do not collect your 25 information, but the user thinks incorrectly that,</p>	87	<p>1 so. They only share contact information for specified 2 and very narrow purposes. 3 So, as regards to deletion, users 4 predominantly expect their websites to allow deletion of 5 the collected data, but websites generally do not allow 6 that. 7 So, there can be other types of mismatches as 8 well. One example is a website-specific mismatch. For 9 example, users do not expect banking websites to collect 10 health information, and most of the banking websites we 11 looked at do not do so; however, there can be specific 12 websites, for example Bank of America, which was one of 13 the websites we looked at, that indeed collect health 14 information. So, you can see this is a mismatch that is 15 specific to a certain website. 16 So, based on the results of our study, we 17 could come up with notices that have less amount of 18 information than a full notice. For example, we looked 19 at 17 data practices. A notice could show information 20 about all 17 data practices, or we could show 21 information about data practices where there's a 22 mismatch between what users expect and what websites do 23 or actual data practices of websites. 24 So, for example here, for the Bank of America 25 privacy notice, there were mismatches for 11 data</p>
86	<p>1 indeed, the website is collecting their information. So, 2 in this case, the user may decide not to use the 3 website, in which case the user may lose the utility but 4 not privacy. 5 So, some results. So, we have looked at 6 different types of website characteristics, and we found 7 that only website type had a statistically significant 8 impact, and the type impacted users' expectations only 9 for financial and health information, but not for 10 contact or current location information. 11 Several user characteristics also had a 12 significant impact on what users expected. So, for 13 example, users' age impacted whether they expect 14 websites to allow deletion of data. 15 So, now, here I present two examples of 16 mismatches that we found. This one is a mismatch in 17 collection data practice, and this is an example of a 18 yes/no mismatch. So, websites can collect users' 19 information, even when users do not have an account on 20 the website. However, users do not think that happens, 21 or they do not expect that data practice. 22 Now, compare this with a no/yes mismatch, and 23 this is a mismatch in sharing data practice. Users 24 expect that websites will share their contact 25 information for any purpose; however, websites do not do</p>	88	<p>1 practices out of the 17. So, that's -- if you show only 2 11, that would be about 35 percent reduction in the 3 amount of information that the user has to read and 4 process. 5 We could also just show information about 6 mismatches that are more privacy invasive from a user 7 standpoint. For example, I talked about the yes/no 8 mismatch versus the no/yes. If we find that the yes/no 9 mismatch is more invasive, we could only show 10 information about those mismatches, and in the case of 11 Bank of America, it's only five data practices for which 12 there's a yes/no mismatch. So, that would be 70 percent 13 reduction in the amount of information shown in the 14 notice. 15 However, the caveat here is that we do have to 16 go ahead and test with users how effective the shorter 17 notices will be, and -- yeah. 18 So, as part of future work, we are planning to 19 also study expectations in the desired sense, and 20 compare that with expectations in the likelihood sense, 21 and may also compare both of them to actual data 22 practices of websites. 23 We are also, as I mentioned, we will test the 24 effectiveness of notices that highlight mismatched 25 expectations and see whether they actually reduce user</p>

89

1 burden and see whether users can make better privacy  
2 decisions.

3 Yeah, that was all. Thank you.  
4 (Applause.)

5 MS. ANDERSON: Thank you, Ashwini.

6 Next we'll hear from co-presenters Heather  
7 Shoenberger of the University of Oregon and Jasmine  
8 McNealy of the University of Florida. They will be  
9 presenting on reasonable consumer standards in the  
10 digital context.

11 MS. McNEALY: So, good morning and thank you  
12 for having us. Our project is online or -- offline  
13 versus online, re-examining the reasonable consumer  
14 standard in the digital context. The impetus for this  
15 project is really trying to get a deeper understanding  
16 of how consumers act when online.

17 So, we know from prior literature that people,  
18 individuals, act differently, supposedly, offline than  
19 they do online. So, we wanted to take this into a  
20 further exploration of consumers. And we know that the  
21 reasonableness standard is a standard that is used for  
22 regulators, for example, in assessing complaints related  
23 to deception. So, we wanted to find out more and  
24 explore this a bit more.

25 So, we came up with an umbrella project that

90

1 used mixed methods to examine this question. One of the  
2 first things we did was start to interview. We did  
3 qualitative interviews, and just to skip forward a  
4 little bit, so we asked our interviewees questions  
5 related to how they behave both online and offline, and  
6 we have this quote from an interviewee who we asked  
7 questions related to their expectations related to  
8 privacy or how their information would be used and how  
9 they attempt to control their information.

10 So, when we asked about whether or not they  
11 showed photos offline, if they just met a person, so  
12 it's a stranger, they invite them into their home, and  
13 they break out their family photo album. We asked about  
14 that. And the interviewee said, you know, I would wait  
15 for a friendship to develop offline before showing any  
16 photos to someone in person, but this seems almost  
17 diametrically opposed to what they do when they  
18 participate on, say, Facebook or Instagram, right?

19 But more importantly than just showing photos,  
20 we asked the question about whether or not they would  
21 sign a printed contract without actually reading the  
22 terms of the contract, versus whether or not they always  
23 click yes or no to the terms and conditions of using  
24 various websites, whether it's social media or shopping  
25 or whatever the case may be. So, we wanted to find out.

91

1 So, we noted that there were some significant  
2 differences indicated with respect to their sharing  
3 behaviors, both online and offline.

4 So, to go back a little more about our method.  
5 So, again, we used qualitative and quantitative methods.  
6 So, just some breakdowns for our interviews. We had 30  
7 participants. We did these long-form qualitative  
8 interviews, and we are going to do more long-form  
9 qualitative interviews as well.

10 So, we had 20 women, 10 men. We note the  
11 average age was around 26, and then we have some racial  
12 demographic data broken down as well. Then for our  
13 quantitative side, we did a survey, and we're going to  
14 talk a bit more about the results of the survey today,  
15 and there were 871 participants. Almost equal breakdown  
16 between men and women, but note the age. So, we had an  
17 age of 35.9, so almost a 10-year age difference on the  
18 survey, the qualitative side, and again, the breakdown  
19 of racial demographics.

20 Also important are some of the variables that  
21 we used or we attempted to measure in our survey. These  
22 variables we got from prior literature. They also  
23 emerged, again, when we were doing our qualitative  
24 interviews, and one of those important ones was social  
25 trust. Social trust was measured on a six-item scale,

92

1 and social trust is really asking the participants, you  
2 know, how they felt about whether or not they trusted  
3 that the institutions, the entities, you know, brands or  
4 advertisers, the government, news media, also, how they  
5 felt that they would -- whether or not these entities  
6 would fulfill their responsibilities related to the  
7 consumer's private information.

8 And, so, those are example questions on here  
9 as well. And then the second important variable we  
10 attempted to measure on a four-item scale was control,  
11 or how participants perceived they had control over  
12 their information.

13 So, an example question was, I can use online  
14 privacy tools to remain anonymous online. Perhaps more  
15 importantly are our main dependent variables, so we had  
16 the always click yes. So, again, we're assessing  
17 behavior, whether or not the participant always chose to  
18 click yes related to privacy policies or terms and  
19 conditions online.

20 And the second one was privacy concern was --  
21 we measured on a three-item scale about whether data  
22 companies -- whether they thought that data companies  
23 would collect information about them that would make  
24 them feel uncomfortable.

25 And Heather is going to come and talk about

93

1 some of the relationships we found.  
 2 MS. SHOENBERGER: Right. So, we diverge a  
 3 little bit here, where we're very positive about our  
 4 findings. And also I wanted to note -- well, I'll note  
 5 that in a second.  
 6 So, our always clicking yes variable was our  
 7 indication of behavior, as our DB. This was a  
 8 hierarchical regression, and I made it very simplified  
 9 for this, because we are under a time limit. The first  
 10 block was demographics. The only demographic in this  
 11 particular equation that was significant was age, and  
 12 it's no surprise that it's younger people that predicted  
 13 always clicking yes. We've seen this in numerous  
 14 reports where younger people tend to be a little bit  
 15 more careless online, maybe a little bit more apathetic,  
 16 et cetera.  
 17 Then we moved to a second block, and these are  
 18 two variables that did come up in our surveys and also  
 19 have been used in numerous studies before ours, and  
 20 social trust in this particular case was not a  
 21 predictor, but control efficacy was. So, even though  
 22 they may not actually be able to control their data, the  
 23 belief that they can predicted always clicking yes, and  
 24 we believe this is the result of the confidence that  
 25 people have if they believe they have control, and as a

94

1 result they go ahead and say, sure enough, I'm just  
 2 going to go ahead and click yes because I'm confident  
 3 and I trust that this is going to work out for me.  
 4 Those who had had -- oh, so the next block  
 5 were all items that were derived from our interviews.  
 6 Of course, some of them you've seen in previous studies  
 7 as well, but all of them were derived from our  
 8 interviews.  
 9 So, negative experience, those who had had  
 10 fewer negative experiences, self explanatory, but more  
 11 likely to click yes without reading any terms of  
 12 agreement, no further investigation. Peer  
 13 recommendations, we were really hopeful that a peer  
 14 recommendation would kind of be an if/then rule, if a  
 15 peer recommends Snapchat to me, I would go ahead and  
 16 download it. That was not the case in our regression  
 17 analysis. It wasn't significant.  
 18 Convenience was a pretty big variable made up  
 19 of items like that policies are too long, they take --  
 20 it's faster to just skip them. They're full of  
 21 legalese. Some of the information that we heard last  
 22 night at the conference about how these policies are  
 23 just laden with too much material for consumers to  
 24 ingest, especially in an over-saturated environment with  
 25 jobs and time constraints, et cetera.

95

1 And then the two variables that are really  
 2 important to us for this study were both essentially  
 3 cues. One was site appearance. If the site appeared to  
 4 be safe and not weird, it didn't raise any skepticism.  
 5 Again, we've seen this in previous studies, but our  
 6 participants noted this in interviews as well, predicted  
 7 clicking yes if this looked safe and also was familiar.  
 8 And then just simple presence of a privacy  
 9 policy or an icon like TRUSTe also predicted clicking  
 10 yes. So, this was our behavior.  
 11 And at the conclusion of this, we thought,  
 12 we're on the right track here, these cues are what is  
 13 driving the motivators of actual behavior online, and we  
 14 were really excited.  
 15 Then, we got even more excited for our privacy  
 16 concern variable, a variable that has been heavily  
 17 researched in this area. Many researchers have noted  
 18 the -- and this panel, the panel before us noted that  
 19 there is a disconnect between privacy concern and actual  
 20 behavior. We may have a potential to bridge that with  
 21 this research.  
 22 So, in the -- hierarchical regression is in  
 23 the exact same format, higher ages and higher education,  
 24 again, no surprise, predicts privacy concern. Lower  
 25 social trust, trust of the institutions, predicted

96

1 privacy concern, lower control efficacy, both in line  
 2 with previous research.  
 3 People who had suffered more negative  
 4 experiences were more likely to say that they had higher  
 5 privacy concern. Again, peer recommendation, we had  
 6 high hopes for that, but it didn't work out. Convenience  
 7 fell out of this model as a result of the two cues at  
 8 the bottom, and there are definitely, within the same  
 9 direction as before, if the site had poor esthetics, and  
 10 it was ugly or weird, it made people feel more  
 11 skeptical, predicted privacy concern. And then a lack  
 12 of privacy policy or a link or an icon predicted privacy  
 13 concern. And note that both of those two cues predicted  
 14 both the concern and the behavior.  
 15 So, in this study, our aim was to better  
 16 define the behavior of the average consumer online, and  
 17 it appears that while they're not -- they're  
 18 specifically not reading policies, especially when these  
 19 safety cues exist. So, it leads us to have the same  
 20 conversation that the rest of our panel has had, where  
 21 if they're not reading the policies, can there be  
 22 meaningful notice and choice? Of course, that's a  
 23 question for potentially another day.  
 24 And if we make really clever use of the cues,  
 25 and there may be more than the ones that we explored,

<p style="text-align: right;">97</p> <p>1 both entities who collect data, so businesses,  2 advertisers, the government, news media, who use data,  3 can reduce privacy concern, which is something that they  4 would like to do, encourage the free flow of data,  5 another something that they would like to do and  6 something that last night was mentioned that the Federal  7 Trade Commission potentially may be interested in doing,  8 also, and increase trust.</p> <p>9 And on the flip side of that, consumers could  10 rely on cues that are more uniform and meaningful, even  11 if they don't read the privacy policies that underlie  12 those particular cues.</p> <p>13 So, with that, now I really have to move  14 through this very quickly. So, there's really a  15 three-prong approach, and we have already begun the  16 research to sort of decide whether or not this is the  17 right approach, but we would like to suggest guidelines  18 for different types of data collection and use,  19 something that has been echoed on the panel already,  20 based on the average consumer's expectation of privacy.</p> <p>21 So, there is some additional research to do,  22 and then delineate those types of data collection and  23 assign a cue, or a heuristic to each type of data that  24 would be endorsed by the FTC. Here is the catch for  25 people who are in the advertising industry who are in</p>	<p style="text-align: right;">99</p> <p>1 everybody. Examine some additional contextual variables  2 as they arise, because while the cues that we mentioned  3 are really good predictors, they may not be the only  4 ones.</p> <p>5 Design policies for readability and  6 understanding for consumers so that they have the  7 opportunity to make meaningful choices if they do, in  8 fact, read those. And, finally, something that we think  9 is really important, and I will diverge for just a  10 second, literally just a second, in Australia, there was  11 a really great PSA to help people avoid being hit by  12 trains, it's called Dumb Ways to Die, and it's gone  13 viral and has actually resulted in lower train deaths,  14 and it's really a silly video.</p> <p>15 You can look it up on YouTube, there's these  16 little people or little animal type things dancing  17 around and talking about dumb ways to die and don't get  18 hit by a train. And essentially, we're looking to do a  19 PSA like that, that would be based on research in  20 America, I mean, that worked in Australia, it may not  21 work here, to allow both the consumers to understand  22 what these icons mean, how they can use them as a way of  23 increasing trust, and how -- and also to entice entities  24 to go ahead and opt into this system and adopt the  25 guidelines the FTC has put forward in a way to align</p>
<p style="text-align: right;">98</p> <p>1 the business of collecting and using consumer data.  2 They would have to adhere to those guidelines in order  3 to use the cue on their sites, which would signify  4 safety, increase trust, hopefully, et cetera.</p> <p>5 So, we would also do research on what icons  6 would be most effective to consumers, and also link  7 those icons to readable policies. Another thing that we  8 noted was the convenience variable was made up of items  9 like it's too long, it's full of legalese, we don't  10 understand, and if we could make those policies readable  11 and approachable to the consumer, something that we can  12 do in the lab, we can test this, we could potentially  13 also for that small sect of people who are going to read  14 those policies, they at least will have the opportunity  15 to make meaningful choices, and it will be short, quick,  16 and more concise.</p> <p>17 So, in conclusion, we are continuing to  18 pinpoint consumer expectations of privacy in a way to  19 develop these guidelines and the resulting cues that  20 would align with the guidelines. As Jasmine mentioned,  21 we are continuing to collect data both in the interview  22 portion of the study and also in the survey, just to  23 make sure that we have as close to a census as possible,  24 because we are dealing with the average consumer in the  25 United States, and we want to make sure that we get</p>	<p style="text-align: right;">100</p> <p>1 with consumer expectations.  2 And with that, we conclude.  3 (Applause.)  4 MS. ANDERSON: Thank you very much, Heather  5 and Jasmine.</p> <p>6 Our final presentation is by co-presenters  7 Anelka Phillips of the University of Oxford and Jan  8 Charbonneau of the University of Tasmania. I think you  9 two win for the longest commute today. And Anelka and  10 Jan will be presenting their work on privacy in the  11 direct-to-consumer genetic testing space.</p> <p>12 MS. CHARBONNEAU: Well, first off I would like  13 to thank the FTC for the opportunity to discuss our  14 research. We're going to talk about privacy of a  15 specific type of data, that being genetic data, the data  16 that results from genetic testing. So, a very specific  17 type of data.</p> <p>18 What we have to realize is, genetic data is  19 the most personal data there is out there. Not only is  20 it a unique identifier of us individually, but because  21 of the familial nature of DNA, it can also identify our  22 families. So, when we're talking about privacy in this  23 context, we're talking about it in a much broader  24 context, not just personal, but looking at the family.  25 We also know that this data is inherently</p>

101	<p>1 identifiable, okay? There's growing recognition that it 2 is simply not possible to de-identify this data in a way 3 that makes it impossible to re-identify it. It may take 4 a good skill set, but as we get increasing numbers of 5 genetic databases out there, as there are more public 6 databases, we know that we can re-identify that data. 7 The other thing is, this data is irrevocable. 8 If there's been a privacy breach, you can't change it. 9 It's not like your iTunes password, you can't come up 10 with another one. Okay? So, this is a different type 11 of data. 12 Does it matter if this happens in a 13 direct-to-consumer genetic testing situation? Well, the 14 first thing we have to realize is the difference between 15 traditional genetic testing and what happens when we 16 have genetic testing in a direct-to-consumer setting. 17 Traditionally, genetic testing has happened 18 within a country's health care system, and that's 19 important because when an individual gets a genetic test 20 in their health care system, they're deemed a patient. 21 And by being called a patient, that enlivens a whole 22 host of professional and regulatory oversight, existing 23 legal duties of care, and simple things like 24 doctor/patient confidentiality. So, all the government 25 systems for data protection of health care kick in,</p>	103	<p>1 health-related research as opposed to commercial. 2 We've also modeled the DTC space, and that was 3 an interesting exercise, and forced the thinking to go 4 broader than just the consumer/company interaction. What 5 we realized very quickly was not only does DNA go a lot 6 of places, that sample travels from labs to companies 7 and who knows where, through the postal system, usually, 8 but also those results can go places. Okay? The actual 9 genetic data about those individuals gets spread around. 10 And that informed the research that I'm going 11 to talk about today, which is an online panel of 3,000 12 respondents of a thousand American, a thousand 13 Australian, and a thousand UK respondents. We've just 14 added in a thousand Japanese respondents, which will 15 give us some interesting contrast. 16 The way the sample broke down, about 10 17 percent of the people are actual consumers, and that 18 equates to those early adopter categories. That leaves 19 about 90 percent of my respondents who are the potential 20 consumers. So, we're able to look at actual versus 21 potential consumers. 22 So, what does privacy mean from the general 23 public's perspective? Well, simply stated, if something 24 is private, it's not shared; if it's shared, it's not 25 private. Okay? The simple way. And that's how the</p>
102	<p>1 because that's a patient. 2 When we look at direct-to-consumer genetic 3 testing, we have to realize that at its core, this is a 4 commercial transaction that occurs in each country's 5 marketplace, and increasingly in market space, because 6 the majority of the activity is actually online. 7 When an individual engages with DTC, they 8 engage as a consumer. What that means is that enlivens 9 each country's consumer protection legislation. It also 10 enlivens some particular legal protections in contract, 11 negligence, et cetera. Okay, but a very, very different 12 situation. 13 What does the general public think of when 14 they think of privacy? At the Center for Law and 15 Genetics at the University of Tasmania, we've been 16 looking at genetic privacy issues for the last 20 years, 17 and in the last few years, we've moved into DTC. Some 18 of our early research in direct-to-consumer genetic 19 testing suggested from the Australian general public's 20 perspective that privacy concerns were going to be the 21 key constraint on commercial uptake. 22 Interestingly, this past year, we found the 23 same results when it comes to intention to biobank, in 24 other words giving a genetic sample into a genetic 25 database for nonprofit, institutional, and</p>	104	<p>1 general public looks at these things. 2 Privacy issues arise from sharing. So, 3 privacy is all about control over sharing. Providing 4 your permission to share means that you have control 5 over your privacy. So, that's the way the general 6 public looks at it. If my permission is asked, then I 7 know what's being asked for, I have the opportunity to 8 ask questions, but I also have the opportunity to say 9 no, and that my no will be respected. So, I have 10 control over my privacy if my permission is sought. 11 So, what do consumers think about whether or 12 not their permission will be sought? In other words, as 13 the previous presenters alluded to, this area of 14 perceived control. Well, interestingly, the American 15 respondents, 47 percent, thought they had perceived 16 control. And what's interesting is, on any dimension 17 that I analyzed on, Americans are statistically 18 different to the other consumer groups. 19 For the UK, it's 43 percent; for Australians, 20 it's 40 percent; and for Japanese, it's 36 percent. So, 21 that's quite a difference in terms of whether or not 22 people think their permission is going to be asked. Are 23 they in perceived control? If they are in perceived 24 control, what does that mean? Well, they're more likely 25 to purchase the DTC tests. They're more likely to</p>

105	<p>1 participate in DTC research. And that's important</p> <p>2 because that's permission-based, right? They asked</p> <p>3 their permission, but do they actually realize that what</p> <p>4 they're doing is giving nonspecific enduring consent?</p> <p>5 They're also more likely to share broadly.</p> <p>6 They'll share with family, not friends, so there's some</p> <p>7 control. They'll share with their doctors, and that's</p> <p>8 important because DTC companies very clearly state their</p> <p>9 results are for recreation, education, or information</p> <p>10 only; they are not a diagnosis. But as Graeme Suthers</p> <p>11 said, it would be a very brave GP who would action a DTC</p> <p>12 test.</p> <p>13 If they go to their doctors, they're back into</p> <p>14 the traditional system. They're also more likely to</p> <p>15 engage with online sharing communities. But does</p> <p>16 perceived control equate to actual control? These are</p> <p>17 commercial transactions governed by contracts and</p> <p>18 privacy policies. We did some research in Australia,</p> <p>19 looking at the privacy policies of the DTC companies</p> <p>20 operating there. Do they comply with our legislation?</p> <p>21 The short answer, no, they do not.</p> <p>22 I'm now going to hand it over to Andelka to</p> <p>23 talk more about contract terms.</p> <p>24 MS. PHILLIPS: Well, I've actually been</p> <p>25 looking at the contracts and privacy policies of</p>	107	<p>1 blindness online, so they may just not notice things, we</p> <p>2 may not read them, we just click on "I agree." And this</p> <p>3 is really problematic in this context, and I think there</p> <p>4 really needs to be reform, because unlike some of the</p> <p>5 other what was said that consumers don't read these,</p> <p>6 I've had to read 71 contracts, and I really think that</p> <p>7 there are problems here.</p> <p>8 So, the major privacy risks in this context</p> <p>9 arise chiefly from sharing or sale of sequence DNA, but</p> <p>10 also from sharing or sale of other types of personal</p> <p>11 data, often health data or other data that we might</p> <p>12 normally consider to be sensitive.</p> <p>13 This is because companies are often engaging</p> <p>14 in ongoing health research, so they're collecting large</p> <p>15 amounts of personal data from consumers. There is also</p> <p>16 the risk of possible discrimination based on a person's</p> <p>17 genetic makeup.</p> <p>18 And then there are some other risks that</p> <p>19 arise. Some of these are more future risks, so there's a</p> <p>20 possibility with the increasing use of biometrics that</p> <p>21 in the future these genetic databases could be used for</p> <p>22 identity theft, targeted marketing, the most obvious</p> <p>23 example at the moment is targeted marketing of drugs to</p> <p>24 particular population groups or even family groups.</p> <p>25 Also there's a potential for discrimination in</p>
106	<p>1 direct-to-consumer tests for companies that offer tests</p> <p>2 for health purposes. Now, as has been noted in the</p> <p>3 previous session, and also in the previous group's work,</p> <p>4 these contracts and privacy policies appear everywhere</p> <p>5 online, basically any website you use, any software</p> <p>6 update you make will be subject to terms and conditions,</p> <p>7 and they'll be presented either as terms and conditions,</p> <p>8 terms of use, terms of service, privacy statements,</p> <p>9 privacy policies, and sometimes in this context they're</p> <p>10 combined in one document.</p> <p>11 At present, these are used to gather not just</p> <p>12 the purchase of DNA tests, but also using the website,</p> <p>13 and sometimes participation in any research the company</p> <p>14 is doing.</p> <p>15 Now, as several people have previously noted,</p> <p>16 people don't tend to read these contracts and privacy</p> <p>17 policies, partly because there are just so many, and it</p> <p>18 would take too long. This industry is no exception to</p> <p>19 that, and I would also say that similarly to most</p> <p>20 e-commerce, these contracts are also not</p> <p>21 industry-specific, so they don't necessarily address all</p> <p>22 the issues raised by the industry and what they're doing</p> <p>23 with data.</p> <p>24 And because of the ubiquity of these</p> <p>25 contracts, consumers often also display inattention or</p>	108	<p>1 employment or insurance, if this data is shared</p> <p>2 inappropriately. And, more remotely, there's the risk</p> <p>3 of creating synthetic DNA.</p> <p>4 Now, as I previously noted, these contracts</p> <p>5 are not industry-specific, so often you'll encounter the</p> <p>6 same terms in these contracts that you would when</p> <p>7 purchasing a product or downloading a song online. And</p> <p>8 they also use really similar wording.</p> <p>9 Now, in the United Kingdom and the European</p> <p>10 Union, there is strong consumer protection legislation</p> <p>11 that deems some terms in consumer contracts to be unfair</p> <p>12 and unenforceable, and at present, some of these terms</p> <p>13 would likely be deemed unfair and unenforceable. And</p> <p>14 this is interesting because I know I'm at the Federal</p> <p>15 Trade Commission's conference, but I've been looking at</p> <p>16 mainly American companies, this is an American industry</p> <p>17 overwhelmingly, but these tests are sold</p> <p>18 internationally, and people's samples are being sent</p> <p>19 across borders, and, so, there is a need for</p> <p>20 international collaboration to protect consumers in this</p> <p>21 context.</p> <p>22 So, one of the most concerning things here is</p> <p>23 that consent will often be deemed through use or viewing</p> <p>24 of a website, and often consent to altered terms will</p> <p>25 also be deemed through continuing to use the website.</p>

109

1 Now, as most of you are aware, it is often  
2 easy to use a website without ever looking at the terms  
3 and conditions. So, this is quite concerning, because  
4 the other thing that's very common, and the majority of  
5 companies will include this, and 39 percent of companies  
6 include a clause that allows them to change their terms  
7 at any time. And only a very small percentage, around  
8 six percent, will actually -- or it might actually be  
9 four percent, I'm sorry -- yeah, six percent, will  
10 notify a person directly by email of changes.

11 So, most of the time, companies can change  
12 their terms at any time or from time to time, without  
13 direct notice to the consumer. And this is important  
14 here because it could have an impact on what companies  
15 do with your data. They could change their policies on  
16 sharing, sale, or storage of data, and this can  
17 significantly impact consumers.

18 As Jan mentioned previously, too, because this  
19 is marketed as a consumer service, companies are often  
20 including clauses that say that their services are only  
21 for research, informational, or sometimes even  
22 recreational purposes. Now, in the context of health  
23 testing, I would question whether anyone orders a breast  
24 cancer risk test for recreational purposes.

25 And skipping on, quite a few of them also

110

1 share data with law enforcement, which consumers may not  
2 be aware of, and there's often very broad sharing with  
3 potential third parties that might include affiliates,  
4 and -- yes, I'm running out of time -- but I really do  
5 think there's a need to improve these contracts. And  
6 following on from the previous two discussants' work, I  
7 really think these contracts need to be written in a  
8 more easily understood way that would enable consumers  
9 to make informed decisions.

10 So, thank you very much.

11 (Applause.)

12 MS. ANDERSON: Thank you, Anelka and Jan.

13 So, now it's time for our discussion session.

14 We'll be spending about 20 minutes, which I'll be  
15 leading with my co-discussants, Alan McQuinn of the  
16 Information Technology and Innovation Foundation, and  
17 Darren Stevenson of the University of Michigan and  
18 Stanford Law School.

19 So, I'll just start us off. We're each going  
20 to provide some brief comments about what we have heard,  
21 and then we will ask the presenters about their work and  
22 its implications.

23 So, first, to me it seems like you are all  
24 striving to answer some of the same basic questions. So,  
25 what do consumers think about privacy and why? And

111

1 those include things like what are their expectations  
2 and hopes about the kind of data that's going to be  
3 collected and how it's going to be used, how much  
4 control do they have, what affects their understanding,  
5 what affects their willingness to trade privacy  
6 consciously or subconsciously, or unconsciously, for  
7 some benefit, and is that contextual, does it vary by  
8 the trust of the firm or online effects.

9 And I noticed three common themes in your  
10 answers or your findings. The first is that notice  
11 seems to be failing. So, Anelka and Jasmine's paper  
12 talked about the ubiquity of form contracts and how  
13 companies have begun to incorporate crooked clauses that  
14 don't seem to be related to the purpose of the contract  
15 from the consumer's perspective, but do give the company  
16 whose policy it is some sort of an advantage.

17 Serge found that about 75 percent of  
18 permissions were being requested invisibly. Ashwini  
19 found 40 percent of collection practices that she was  
20 looking at in her study were not addressed or were  
21 unclear in the privacy policies. Ashwini, Heather, and  
22 Jasmine found that consumers were relying upon things  
23 other than privacy policies to decide whether they are  
24 going to use an app, and even to form their expectations  
25 of what's happening.

112

1 The second theme is that companies' policies  
2 and practices aren't matching up with consumers'  
3 expectations. Ashwini found rampant mismatches between  
4 expectations and reality, Anelka and Jan found that  
5 half of DTC companies' policies allowed them to share  
6 consumers' personal information with third parties,  
7 contrary to what consumers would have expected, Serge  
8 found consumers would rather not allow so much access to  
9 their data.

10 And the third theme was that several of you  
11 were recommending that companies highlight unexpected  
12 data collection and use, especially when it involves  
13 sensitive information. Serge was recommending runtime  
14 prompts and indicators when apps were accessing  
15 protected resources, Ashwini recommended highlighting  
16 unexpected uses, Anelka and Jan were recommending  
17 highlighting key clauses and providing shorter, clearer  
18 notices.

19 Now, one of the biggest benefits that I see of  
20 PrivacyCon is that it brings all of you together, the  
21 best and the brightest, all working to understand the  
22 same issues and providing us with the benefits of your  
23 learning.

24 So, we are hoping that this conference is  
25 going to facilitate you learning from and building upon

113

1 each other's work, and I hope that we can continue to  
2 benefit from the insights that you have given us about  
3 how best to protect consumers' privacy, and industry can  
4 hopefully do the same.

5 As Chairwoman Ramirez said, it's now more than  
6 ever that we need to stay up to date with the latest  
7 findings on privacy and data security research in order  
8 to fulfill our mandate to protect consumers, and your  
9 efforts deepen our understanding of our own research in  
10 that respect.

11 So, thank you all again for coming, for  
12 sharing your work and your thoughts, and with that I am  
13 going to turn it over to my co-discussants for their  
14 thoughts and allow them to ask first questions.

15 MR. McQUINN: Thanks, Kristen. Thank you to  
16 the FTC for letting me come here today and respond.

17 I thought that the all of the presentations  
18 were very thought-provoking and they could definitely  
19 help businesses better understand their consumers. Now,  
20 but we're here today at the FTC, and what I'm looking  
21 for is evidence of the need for public policy  
22 intervention. And, frankly, I'm not sure that there is  
23 much.

24 As we walk into this, there's definitely a lot  
25 of discussions over different public expectations versus

115

1 think what we have here is we have evidence, empirical  
2 studies that show that consumers have expectations. All  
3 of you in this room, you guys are not ordinary  
4 consumers, because you're here at PrivacyCon, but  
5 ordinary consumers we're seeing that there are  
6 consistent measurable expectations.

7 I really enjoyed the studies and I encourage  
8 you all to read them if you have not read the papers.  
9 And I think most of these papers have supported this  
10 notion of contextual integrity that's popularized by  
11 Nissenbaum and others, but the idea that pre-held  
12 expectations are measurable and can be demonstrated.

13 Two complications come to mind. So, the first  
14 is the difference between expectations and preferences.  
15 It was clear in Ashwini and colleagues' papers, they  
16 were really careful to define what is an expectation.  
17 What are we actually studying here, and then to contrast  
18 that with consumers' preferences. Expectations being  
19 different than preferences, which we saw in Turow's  
20 work, and with his colleague, that consumers might just  
21 be resigned, so that where expectations and preferences  
22 converged, I think this is a very fruitful area of  
23 study.

24 So, what are we measuring when we are  
25 measuring consumers' expectations, is it what they are

114

1 privacy, or people not understanding the legalese in  
2 direct-to-consumer genetic contracts, but is that a  
3 public policy problem? I'm not so sure.

4 Let me draw an analogy. Say I'm not  
5 necessarily sure what goes into my Chipotle burrito.  
6 Sure, I'm able to pick different fillings and -- I may  
7 be able to pick different fillings, but I'm not so sure  
8 how they're sourced. So, when you ask me questions  
9 about what's in my Chipotle burrito, my expectation may  
10 differ from the reality of what's in there.

11 Now, that's not necessarily a public policy  
12 problem, right? But what is a public policy problem is  
13 when consumers start to get sick or have food poisoning  
14 as a result of the contaminated food from the Chipotle  
15 burrito, but when I'm listening to these presentations  
16 and reading these reports, I'm not necessarily -- I'm  
17 seeing that we're talking about what's in the privacy  
18 burrito, rather than actually talking about the privacy  
19 food poisoning. That's just some food for thought, I  
20 guess. And I look forward to a good discussion.

21 Thank you.

22 MR. STEVENSON: I have no way to connect to  
23 the burrito, but we wish Chipotle well with their  
24 current issues.

25 So, at the risk of stating the obvious, I

116

1 just resigned to give up, or is it what they would  
2 prefer? And in the papers, a few of them kind of went  
3 back and forth on that.

4 A second complication that comes to mind are  
5 expectations or preferences or we'll just say consumer  
6 tastes. This is a moving target, so these are  
7 continually changing, so even though they're consistent  
8 and we can measure them empirically and the FTC can  
9 decide does it warrant intervention based off of trend,  
10 these are evolving and they change over time.

11 So, how can policy, which tends to move  
12 slowly, track and be responsive to something that is  
13 changing, that is dynamic? So, if we were to have  
14 PrivacyCon in three years, next year, five years, and we  
15 repeat all these studies of consumers, would we see the  
16 same expectations. So, how can policymakers incorporate  
17 this sort of moving target of consumers' expectations?

18 So, I look forward to our discussion here and  
19 we can open it up to questions. Or if you have any  
20 responses to our comments.

21 MS. McNEALY: I like the burrito analogy, but  
22 at the same time, if Chipotle has lean steak or whatever  
23 they have, right, they -- I mean, if they make  
24 representations to the consumer that it's from a certain  
25 source, then you have expectations that, hey, my beef is

117

1 from a certain source, and even if we don't know exactly  
2 where it's from, we have an expectation that we should  
3 get at least a product of some I guess quality, or at  
4 least we expect the regulators would enforce them, you  
5 know, would enforce the restaurant giving us a product  
6 that either won't make us sick or won't have been, you  
7 know, had something done to it by a worker there, right?

8 So, I think there is a certain level of  
9 protection we expect from regulators with respect to  
10 things particularly like privacy. Just I think most of  
11 us are used to jaywalkers, right? So, we're supposed to  
12 cross at the light, right? But jaywalking is more  
13 convenient. It just is. But there is an inherent risk  
14 in jaywalking, right?

15 So, regulators, particularly on, say, college  
16 campuses, which I think most of us are used to, have  
17 said, you know what, we see people are just going to cut  
18 across here anyway, so because there is a power dynamic  
19 that skews in favor of the moving vehicle, let's put a  
20 crosswalk here and we expect the car, the bus, the  
21 whatever, to stop and let those people who are -- who  
22 would be jaywalking, in the first place, to cross. It  
23 doesn't take away the power of the bus or in this case  
24 the corporation, but it does say, you know, let's quote  
25 Spiderman, with great power comes great responsibility,

118

1 right?

2 So, the expectation is that when the bus or  
3 the whatever sees that person in the walk, they're going  
4 to stop. Does it happen all the time? No, but I think  
5 from a public policy perspective, it's putting in --  
6 it's proactive measures to protect people from  
7 themselves and other people at times.

8 So, I think, you know, from the perspective of  
9 a regulatory agency that is a consumer protection agency  
10 would want to do something proactively when there are  
11 signs of issues or trouble. I think it's perhaps  
12 incumbent upon a consumer protection agency to do that.

13 MR. EGELMAN: So, I guess the issue of  
14 expectations versus preferences. So, we've done some  
15 studies and we have, you know, actual data to show that,  
16 you know, to some extent, this is an issue of learned  
17 helplessness. So, people are just sort of, you know,  
18 resigned to the fact that all of our data is out there,  
19 regardless of whether that is actually the case.

20 So, for instance, we did a study looking at  
21 single sign-on in websites. So, when you click the, you  
22 know, use your Facebook login to log into this website,  
23 those sites can then request some data from your  
24 Facebook profile. And, so, we wanted to see whether,  
25 you know, making that more apparent to users, so trying

119

1 to highlight what types of data might be collected by  
2 those websites from your Facebook profile, we expected  
3 that that would have an effect on whether people, you  
4 know, used this.

5 And we found that that was not the case. And  
6 when interviewing subjects, they said, oh, well they  
7 just assumed that Facebook is giving away all this data  
8 anyway, so I might as well get a benefit from it.

9 And so that's sort of the learned helplessness  
10 issue. And I'm not sure there's anything -- I think  
11 addressing that part of it is sort of putting the cart  
12 before the horse, because I think one of the issues we  
13 need to focus on are the expectations, you know, before  
14 they're formed.

15 Some of that might be doing a better job of  
16 public education with regard to online privacy, other  
17 pieces might come in the form of enforcement making that  
18 somewhat more subjective. So, yes, the law moves very  
19 slowly, technology moves quickly, but I don't think --  
20 you know, I don't think the issue is making the policies  
21 around specific technologies, the issue here is  
22 narrowing or closing the information asymmetry.

23 So, you know, while we don't expect people to  
24 read every privacy policy that they encounter, we have  
25 some expectations about what a business might be doing,

120

1 as was pointed out.

2 So, you know, I don't expect, you know,  
3 regardless of what they say about, you know, what farm  
4 the beef came from, I don't expect it to have E. Coli in  
5 it, and that's not something that they need to  
6 explicitly, you know, provide notice for, it just should  
7 be expected that there's no E. Coli in this beef. I'll  
8 leave it at that.

9 MS. PHILLIPS: I would like to say, because we  
10 kind of ran out of time a little bit, but there is  
11 really a need for more transparency in the industry  
12 we're looking at, because often if you look at website  
13 claims, there will be quite a gap between what the  
14 contract actually says and what the website is  
15 encouraging consumers to believe when they are  
16 encouraging people to purchase tests.

17 And the other thing is that because the  
18 industry is so new and the technology is changing so  
19 fast and it is largely unregulated, a lot of tests that  
20 are coming to market haven't been validated. So, there  
21 is a question sometimes about what the consumer is  
22 actually buying, because the value to the company is the  
23 sequenced DNA, which they are using in ongoing research  
24 often. So, they are selling a product that gives them  
25 very personal data that they use for a long time and may

121

1 not be destroying ever, potentially, and the consumer,  
2 an ordinary consumer doesn't necessarily have the  
3 expertise to understand all of the risks.

4 And the other thing is that genetic test  
5 results are complex in nature, a lot of general  
6 practitioners have trouble interpreting genetic test  
7 results, and there's been some studies that have shown  
8 that a lot of GPs wouldn't be comfortable with  
9 interpreting a DTC test result if a consumer brings it  
10 in, but at the moment, most of the time, it's being  
11 avowed as a consumer service.

12 And in terms of particular worrying terms in  
13 contracts, in some countries like the UK, the Office of  
14 Fair Trading, which is now being disbanded, but is the  
15 competition and markets authority, has a history of  
16 working with industry to try to discontinue certain  
17 unfair terms as well, and that's what I would say. There  
18 are some terms that really shouldn't be in the contract,  
19 because it's making it a very unfair and unbalanced  
20 bargain, and a lot of the use of these contracts is also  
21 eroding traditional contract law principles, really.

22 And I think people will often tend to engage  
23 with these much -- and I think your work shows that much  
24 more differently than they would with a paper contract.

25 So, for browsewrap, which is where the terms

122

1 are on a hyperlink, it's akin to walking into a shop and  
2 being bound by a sign on the wall that you didn't see  
3 and walking out again. And that's really problematic.  
4 Thank you.

5 MR. STEVENSON: I think I will add one. So,  
6 on someone's slide there was a mention of incorrect  
7 mental models, and a lot of us think through consumer  
8 knowledge and I think the educated consumer. So, no one  
9 would argue for an uninformed consumer as the goal, but  
10 I think I want to push back a little bit on that idea  
11 that our goal or the goal of some of this work is to  
12 correct mental models. I'm curious what you guys think.

13 So, someone smarter than me said something  
14 like all models are wrong, some are useful. And I think  
15 the consumers sometimes have very strong or inaccurate  
16 models that are helpful heuristics, and I'm curious if  
17 you guys in this work since you're all studying  
18 consumers' perceptions, if you sort of see those  
19 inaccuracies actually beneficial or -- not that we want  
20 this inaccurate model. Does that make sense?

21 MR. EGELMAN: Yeah, I think that was my slide.  
22 I think that one of the bigger problems with notice and  
23 choice is that I guess there's unreasonableness on both  
24 sides. So, there's, you know, unreasonable expectations  
25 on what the consumer should know to make an adequate

123

1 choice based on the notice given to them, so it's  
2 unreasonable to expect every consumer to read every  
3 privacy policy that they encounter.

4 At the same time, yes, people have really bad  
5 mental models about what's happening with their data  
6 when they go online. And I think, you know, maybe there  
7 needs to be some better outreach on that issue, but at  
8 the same time, I think, then, you know, that goes sort  
9 of to enforcement, which is instead of thinking, well,  
10 did the company give notice and was it incorrect, you  
11 know, and outright misleading, but is it also adding  
12 into that equation, is it reasonable to expect that  
13 someone could actually understand this? And I don't  
14 think that's currently being taken into account.

15 MS. SHOENBERGER: I will also answer that very  
16 briefly. As far as using heuristics, part of the  
17 cognitive advisor sort of mental model, first of all I  
18 disagree that heuristics, using them are faulty. They're  
19 almost always correct. I mean, we rely on them all day  
20 long in various capacities.

21 I think what we were arguing for were  
22 heuristics that were actually giving consumers -- they  
23 were backed by informed and concise and true information  
24 that the FTC approves. And, so, by using -- by  
25 promoting consumers and allowing them to see what these

124

1 heuristics mean, promoting the keys to those consumers,  
2 it gives them a meaningful choice.

3 A heuristic is no longer something that risk  
4 is as much of an issue for, more it is something that  
5 can genuinely grow on them as an indicator of safety.

6 MS. ANDERSON: Heather, can you guys talk a  
7 little bit more about how you see that kind of heuristic  
8 coming into place, how you'd develop it based on an  
9 average consumer's expectation, given that we heard a  
10 lot of the findings are consumer-dependent, and it kind  
11 of depends on your background and the experiences you've  
12 had, your age? How would you go about trying to develop  
13 something that would be generally applicable?

14 MS. SHOENBERGER: Right. We are in the  
15 preliminary stages of doing that, and this would be  
16 something that we would be testing in a lab, probably, a  
17 physiological lab, looking at people's automatic  
18 responses in addition to self-report, but that said,  
19 looking at heuristics and making cues that were in line  
20 with guidelines that we had come up with is based on  
21 consumer expectations of a different type of data  
22 collection.

23 So, we came at it, and this is an arguable  
24 point, from the type of data collection and how it's  
25 being used, and then entities could opt in, depending on

125

1 how they were collecting and using that particular type  
2 of data. So, there would almost be a continuum of the  
3 address that you could or icons or cues that you could  
4 use.

5 And then in order to use that on your site, or  
6 within your materials, you would have to adopt the FTC's  
7 guidelines that went with that particular icon, and we  
8 would empirically test every single element of that.

9 So, the icon itself might be something that  
10 you would have to test to see if it was something that  
11 caught someone's eye, or someone noted that, I think it  
12 was Turow noted that people didn't notice some of the  
13 privacy policies. That's something we could correct  
14 with better web design and better icon design.

15 MS. ANDERSON: Okay. We have about 20 seconds  
16 left, so I would like to give you guys an opportunity to  
17 ask the last question.

18 MR. McQUINN: So, to follow up on what Darren  
19 said, with how privacy concerns kind of have morphed and  
20 changed over time, the ITIF actually released a report  
21 called The Privacy Panic Cycle that kind of tracks this,  
22 but I wanted to see, several different industries up  
23 here have kind of -- that you have studied have changed  
24 over time. Some of them are new like genetic testing,  
25 and Android is on its sixth release. I'm just wondering

126

1 if you could talk about how you've seen expectations  
2 change over time.

3 MS. PHILLIPS: Me?

4 MS. CHARBONNEAU: I think one of the things we  
5 have to acknowledge is that we're moving into the  
6 commercialization of health, and we're moving into the  
7 monetization of health data. And, so, what we've found  
8 is, what's existing at the moment is not  
9 industry-specific, and probably that would be our main  
10 recommendation, that as we move into this, whether it's  
11 direct-to-consumer genetic testing, whether it's the  
12 data that's coming from your Fitbit, whether it's the  
13 information you're putting onto sharing sites thinking  
14 that you're just meeting some folks out there who have  
15 the same complaints you do, and let me tell you what  
16 happened with the latest drug, this is now being  
17 monetized, and this is now in the corporate sphere, and  
18 our protections of the relationships and the data were  
19 created for the traditional health care system. And we  
20 haven't yet made the move over into looking at anything  
21 industry-specific as we move into this new form of  
22 commercializing health care and also monetizing health  
23 data.

24 MR. EGELMAN: So, one thing that we've looked  
25 at is trying to relatively weigh different user concerns

127

1 based on the technologies. And, so, I guess going to  
2 this issue of what policy is needed, and policy moves  
3 slowly and technology moves fast, while people do have  
4 very nuanced privacy preferences and expectations, at  
5 the same time, there are some things that people will  
6 think of as universally bad or universally uninteresting.

7 And, so, we did this study three or four years  
8 ago, we came up with a whole slew of risks related to  
9 smartphone usage, such as an app that uses data for X or  
10 shares data with certain parties, and we had people rank  
11 those. This past year, we did a follow-up study to  
12 that, where we came up with similar risks relating to  
13 wearable devices and IoT, and what we found is, you  
14 know, if you categorize those risks, the results pretty  
15 much held.

16 So, people are almost universally concerned  
17 with things that have financial impact, and almost  
18 universally unconcerned with things that are already  
19 public, such as demographic data that would be publicly  
20 observable. So, you know, an approximation of your age,  
21 for instance.

22 And, so, in that regard, I don't think we need  
23 -- we should expect regulation to be really specific to  
24 the technologies, but we can come up with regulation  
25 around the various risks that most people are concerned

128

1 with, and that should last longer than specific  
2 technologies.

3 MS. ANDERSON: Thank you all. Unfortunately,  
4 we are out of time, even though I feel like we've just  
5 started the conversation, but I do hope that the  
6 conversation continues after this conference. I look  
7 forward to reading more of your research as time goes  
8 on.

9 For all of you in the audience, as you heard  
10 this morning, our cafeteria will unfortunately not be  
11 available for lunch, however there are boxed lunches  
12 that are available for purchase just outside of the  
13 auditorium. They are only taking credit cards. You may  
14 eat your lunch in the overflow conference rooms that are  
15 across the hallway. Food is not permitted in this  
16 auditorium, neither are beverages, except for water.

17 And remember, if you leave the building,  
18 please take time to come back through security on your  
19 way in. If you don't have electronics with you when you  
20 come back through security, that screening will be  
21 faster. You can leave your electronics in this room, I  
22 have been told there is going to be a guard and that the  
23 room will be locked. So, you can do that to try to  
24 expedite your screening on the way back in. And thank  
25 you all for coming, we will see you back here at 1:00

129	<p>1 p.m. 2 (Applause.) 3 (Whereupon, at 12:20 p.m., a lunch recess was 4 taken.) 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25</p>	131	<p>1 being organized by discipline, you know, computer 2 science here, economists over there, the day is 3 organized around the key substantive issues in consumer 4 privacy. This thoughtful organization is leading us 5 towards something that we need for sound privacy policy 6 development. A cross-disciplinary, richly detailed 7 picture of consumers and how they make decisions about 8 technology use. 9 Lurking behind the main regulatory approaches 10 to privacy, whether it's notice and choice, 11 informational self-determination, or a use space model, 12 are questions about individual consumers, their goals in 13 exercising their privacy rights, and their ability to do 14 so in the environment around them. 15 At a high level, I think two principles should 16 guide policy and practice. First, individuals have to 17 be in the loop regarding decisions about what data is 18 collected about them and how it is used; outside the 19 privacy sphere, companies have excelled at helping 20 consumers manage and use highly complex systems. 21 Now, we heard a little bit about Chipotle and 22 the burritos. I actually think a much better analogy in 23 this space would be cars. Cars are now computers on 24 wheels, but we can all drive them, because companies 25 have kept the complexity behind user interfaces that are</p>
130	<p>1 AFTERNOON SESSION 2 (1:12 p.m.) 3 MS. ANDERSON: Next we're pleased to have 4 Commissioner Julie Brill provide a few remarks. 5 Commissioner Brill has long been an advocate for 6 consumers in securing their privacy and data, and we are 7 thrilled to have her here today. 8 Commissioner Brill? 9 COMMISSIONER BRILL: So, thank you, Kristen, 10 and thank you everybody who's here, as well as all of 11 you out in TV land. Lunch may be over, but the feast of 12 scholarship will continue. It's really my pleasure to 13 open the afternoon with a few remarks about the research 14 that's on display here at PrivacyCon, but before I do 15 that, I really have to take a moment to do exactly what 16 Chairwoman Ramirez did, and that is to thank the FTC 17 staff who worked incredibly hard and incredibly well to 18 pull this together. Kristen, Dan, Justin, Maneesha, I 19 know I'm leaving out probably 25 people, but they all 20 did a really, really wonderful job. So, can we just 21 have a round of applause for these fabulous people. 22 (Applause.) 23 COMMISSIONER BRILL: Great job. Now, aside 24 from the quality of projects and presentations, one 25 thing has struck me about today's agenda. Instead of</p>	132	<p>1 simple to use. I think companies can do the same for 2 privacy, but building the right tools depends on 3 understanding which decisions are important to 4 individuals. 5 Second, I'm wary of solutions that depend too 6 heavily on any one technical measure. Now, just as an 7 example, it's a positive development that companies are 8 offering more services that allow individuals to encrypt 9 their communications, and these services are getting 10 more user friendly, but their ease of use is limited to 11 communications that stay within one particular service. 12 If you want to communicate between services, 13 you may be forced to use tools that only a few select 14 experts can really implement properly at this time. But 15 these principles leave many questions open, and details 16 unspecified. What data do consumers expect companies to 17 collect from them? How do they expect companies to use 18 this data? What do consumers understand about what 19 actually happens to their data? Which aspects of data 20 processing should be under consumers' control, and how 21 effective are the tools that companies offer to 22 consumers to exercise this control? 23 Answering these questions requires a 24 three-dimensional approach. So, I was excited to hear 25 this morning from researchers who are using structured</p>

133

1 surveys, qualitative interviews, and looking at human  
2 computer interactions to map out what consumers  
3 understand about the data practices of the services and  
4 devices they use.

5 Of course, it is just as important to  
6 understand more about what happens behind the scenes,  
7 outside the view of consumers. Data and device security  
8 are incredibly important to consumers, yet assessing  
9 security remains well beyond the capabilities of most  
10 consumers, including most of us, but not all of us in  
11 this room.

12 So, I'm thrilled to see researchers doing a  
13 deep dive on security vulnerabilities on specific  
14 Internet of Things devices, while others are analyzing  
15 data from thousands of vulnerability reports to better  
16 understand the kinds of incentives that will spur a  
17 virtuous cycle of discovery, reporting and patching.

18 Also beyond consumers' purview lies the big  
19 data analytics that have developed more quickly than  
20 have frameworks for specific concrete guidance on legal  
21 and ethical issues. Our Big Data report issued last  
22 week is intended as our first step towards providing  
23 such guidance. The report recommends that companies  
24 review their data sets and algorithms to determine  
25 whether they may be having unintended effects, such as

134

1 treating certain populations disparately, and in ways  
2 that may potentially violate the law.

3 Our report also recommends that companies  
4 bring a broad set of fairness and ethical considerations  
5 into their use of big data analytics. The presentations  
6 in the next segment of PrivacyCon address exactly those  
7 issues.

8 Finally, I want to give a shout out to the  
9 institutions that have helped produce the specific  
10 pieces of research that we're hearing about today. They  
11 are just as important as the research itself. Much of  
12 the research presented today comes from universities  
13 that have made substantial, long-term commitments to  
14 examining the relationships among law, technology and  
15 public policy.

16 In addition to generating new research that  
17 also contains policy insights, these universities help  
18 to train students to become leaders in their fields.  
19 Technology-focused centers and clinics have sprouted up  
20 at law schools all over the country in the last decade.  
21 They expose law students to technology, and probably  
22 just as importantly, to the way technologists think.

23 Departments, schools, and even entire campuses  
24 that make interdisciplinary work a core mission are  
25 doing much the same for students of computer science,

135

1 engineering, economics, public policy, and social  
2 sciences. Building these programs has not been easy.  
3 It's often easier to stick closer to traditional  
4 disciplinary lines.

5 So, let me offer a word of encouragement.  
6 PrivacyCon is just one example of the impact that  
7 scientists, lawyers and others can have when they're  
8 trained to do ground-breaking research as well as to  
9 identify and analyze public policy questions and issues.  
10 This combination of research capability and capacity for  
11 action also describes, just coincidentally, the design  
12 of the FTC itself.

13 So, naturally, we are a ready audience for  
14 research that sheds light on the challenges we confront  
15 in enforcement and policy development. And I hope that  
16 the institutions that many of our presenters call home  
17 will be lasting platforms for robust exchange of ideas  
18 with the public and private sectors for many years to  
19 come.

20 So, with that, let's hear what you have.  
21 Thank you very much.

22 (Applause.)

23 COMMISSIONER BRILL: And, Dan, are you going  
24 to -- Dan will introduce the next panelists. Thank you.  
25

136

1 SESSION 3  
2 BIG DATA AND ALGORITHMS  
3 MR. SALSBURG: Thank you, Commissioner Brill.  
4 Could the next panel come on up. So, welcome  
5 back to PrivacyCon. Our first session today really  
6 looked at what kind of data is being collected about  
7 consumers. Our second panel looked at what do consumers  
8 expect is happening with that data, and now, this  
9 session, we're going to look at what actually is  
10 happening with the data.

11 So, I am really pleased to have with me  
12 researchers who are going to present three outstanding  
13 research presentations, and we're then going to discuss  
14 them.

15 So, why don't we get things started with a  
16 presentation from Michael Tschantz and Anupam Datta.  
17 Michael is from Berkeley and Anupam from Carnegie  
18 Mellon, and they're going to lead things off with a  
19 presentation titled Automated Experiments on Ad Privacy  
20 Settings.

21 MR. TSCHANTZ: Thank you. I am Michael  
22 Tschantz, and this is going to be a joint presentation  
23 with Anupam Datta, and we're going to be talking about  
24 AdFisher, a system for looking at online trackers and  
25 determining what information they are using about people

137

1 to select the ads they show to people.

2 There are two things I want you to take away  
3 from this topic. First, it is possible to do this with  
4 scientific rigor, despite not having access to the  
5 internals of the system; and second, we can find such  
6 interesting flows of information, but we can't figure  
7 out why they happened.

8 So, let's get started by motivating the  
9 problem. Here's a web page, it's The Times of India. I  
10 find it an interesting example because it has a lot of  
11 ads from Google on it. Here's two. Now, Google has  
12 little pieces of code across the Internet. In fact,  
13 this web page has two little pieces of code, and these  
14 pieces of code imparts back to Google about what other  
15 web pages you visited. Google can then select the ads  
16 it shows on The Times of India based upon this  
17 information.

18 And this is generally true of online behavior  
19 trackers, there's many trackers with many little pieces  
20 of code all over the place. There's a seemingly endless  
21 number of companies doing this kind of thing.

22 But it can be concerning. I mean, suppose,  
23 for example, you want to show a friend an ad -- a  
24 newspaper article and you see nothing but ads for  
25 antidepressants, which Google may have shown you in

138

1 certain circumstances. Now, Google understands that  
2 people have concerns like this, so they and other  
3 companies have provided things like the ad privacy  
4 settings.

5 Here is a screen shot of my ad privacy  
6 settings, it shows various information inferred about  
7 me. Google got my age correct, but got my gender wrong.  
8 Google also allows you to go in and edit this  
9 information, so if I cared, I could go in there and  
10 provide my correct gender. Google doesn't give us a  
11 whole lot of information about exactly how this thing is  
12 working, however.

13 So, what we have is a situation where we have  
14 our web browsing behavior going into an ad ecosystem at  
15 one end. You have various things like ad settings  
16 sitting in the middle providing sort of a window into  
17 how that ad ecosystem works, providing inferences they  
18 create, and allowing you to put edits in, and then we  
19 see advertisements coming out the other end.

20 But we would like to understand the flows of  
21 information in this system better than they currently  
22 make clear from their privacy policies and descriptions  
23 of how these systems work. And this is a difficult task  
24 because the system is opaque. We don't know what's  
25 going on in that ad ecosystem. Google and other online

139

1 behavioral trackers won't share its source code with us,  
2 we can't do the traditional forms of program analysis.

3 So, we designed AdFisher, a system that allows  
4 us to run experiments on these kinds of opaque ad  
5 ecosystems. Let me run through quickly how AdFisher  
6 works.

7 AdFisher creates a bunch of fresh Firefox  
8 browser instances which simulate users. So, these could  
9 be simulating people who browse various websites. It  
10 randomly assigns them to either a control or an  
11 experimental group. These two groups of simulated users  
12 would display different behaviors on the Internet. They  
13 then interact with the Internet in various ways, and we  
14 collect measurements about how advertisers change their  
15 behavior towards these simulated users.

16 These measurements go into a test of  
17 statistical significance, which reports whether there's  
18 a statistically significant systematic difference  
19 between the experimental and the control group. If so,  
20 we know that whatever information describes the  
21 difference between these two groups, and in how they  
22 behave towards the ad ecosystem, is information being  
23 used by the ad ecosystems to select ads.

24 So, this is our main contribution, is that we  
25 brought the rigor of experimental science to these sort

140

1 of online blackbox experiments in such a way that allows  
2 us to describe cause and effects which are equivalent to  
3 flows of information with the theorem we proofed. It  
4 does it with statistic co-significance, without making  
5 questionable assumptions about how Google operates.

6 This is important because Google is an  
7 extremely complex system, pretty much any assumption you  
8 make about how it's operated might not hold, or perhaps  
9 it holds it for one moment in time but not later when  
10 you're running your experiment. And we provide a high  
11 degree of automation.

12 So, now I'm going to give you an example of  
13 one of the findings we discovered with our system. In  
14 this experiment, what we did was we fired up our  
15 simulated users and we had half of them set the gender  
16 bit to be male and the other half to female on the  
17 Google ad settings page. We then had them all browse  
18 websites related to finding jobs. We then collected the  
19 ads shown to them at The Times of India, and we found a  
20 statistically significant difference in the ads shown to  
21 the male and female groups.

22 Now, this in and of itself isn't terribly  
23 surprising. We know that advertisers show different ads  
24 towards men and women, but what's concerning is the  
25 nature of this difference, something that AdFisher can

141	<p>1 also share with us.</p> <p>2 What we found is that there were a series of</p> <p>3 ads from a career coaching service that was shown almost</p> <p>4 only to the male simulated users. In fact, the ratio</p> <p>5 was so large that it's in violation of the 80 percent</p> <p>6 rule often used in employment law to detect disparate</p> <p>7 impact.</p> <p>8 That being said, we are not claiming that this</p> <p>9 is an instance of illegal disparate impact, because this</p> <p>10 is an ad for a career coaching service, it's not</p> <p>11 actually for a job. Nevertheless, we find this ad being</p> <p>12 shown predominantly to men to be concerning.</p> <p>13 Now, this is just one of the findings. We</p> <p>14 have another interesting one involving substance abuse.</p> <p>15 We found that if you visited a website for a rehab</p> <p>16 center, all of the sudden Google would start showing you</p> <p>17 ads for that rehab center across the web, or at least at</p> <p>18 The Times of India. And this is concerning, since it's</p> <p>19 sort of like medical information being used for</p> <p>20 determining the ads you see on a newspaper's website.</p> <p>21 So, I've used my time to explain some of the</p> <p>22 things we know. Anupam is going to now explain some of</p> <p>23 the open questions left open.</p> <p>24 MR. DATTA: So, I'm very excited about where</p> <p>25 this research area is going in terms of developing</p>	143	<p>1 institution of corrective measures.</p> <p>2 And this is going to involve collaboration</p> <p>3 between computer scientists and legal scholars, and</p> <p>4 probably policy changes. I want to focus only on the</p> <p>5 computer science piece of it for now, but we are working</p> <p>6 on the interaction between computer science and law, in</p> <p>7 part in collaboration with Deirdre Mulligan.</p> <p>8 So, let me highlight some of the nuances of</p> <p>9 assigning responsibility with this concrete instance of</p> <p>10 discriminatory targeting that we found. So, just to</p> <p>11 remind you, this was an instance where typing</p> <p>12 job-related ads were being served in significantly</p> <p>13 higher numbers to simulated male users rather than</p> <p>14 female users.</p> <p>15 So, what are some possibilities here of which</p> <p>16 entity could be responsible? So, one possibility is</p> <p>17 that Google, Google's programmers intentionally</p> <p>18 programmed their targeting system to be discriminatory</p> <p>19 in this way. We considered that to be highly unlikely,</p> <p>20 but nevertheless, it's not something we can rule out</p> <p>21 because we don't have enough visibility or access into</p> <p>22 the system that they use internally.</p> <p>23 Another possibility is that the advertiser,</p> <p>24 the specific advertiser, in this case the Barrett Group</p> <p>25 that was advertising for this career coaching service</p>
142	<p>1 rigorous science and useful tools that are beginning to</p> <p>2 find effects in the ad ecosystem, and more generally in</p> <p>3 online personalization systems. At the same time, I am</p> <p>4 deeply concerned, also, about the findings themselves</p> <p>5 that we and others in this research area are beginning</p> <p>6 to develop, and we'll hear more from the two other</p> <p>7 speakers shortly about other findings.</p> <p>8 These studies are beginning to get a lot of</p> <p>9 attention in the popular press, indicating that these</p> <p>10 concerns are shared much more broadly in the community.</p> <p>11 But there's much more to do in this space. There are</p> <p>12 questions like how widespread are instances of the</p> <p>13 discriminatory targeting or targeting that violates</p> <p>14 privacy expectations of perhaps contextual integrity or</p> <p>15 other notions. And then there is also the question of</p> <p>16 who is responsible?</p> <p>17 So, I want to take a few minutes to highlight</p> <p>18 that these questions are incredibly nuanced to answer in</p> <p>19 the presence of the complexities of data analytics and</p> <p>20 other pieces of an ad ecosystem. So, I'm going to focus</p> <p>21 on this question of responsibility partly because</p> <p>22 following up on the conversations from the morning, I</p> <p>23 think that detection is an important step, but we can't</p> <p>24 just stop there, we have to go towards accountability,</p> <p>25 meaning assignment of responsibility and then</p>	144	<p>1 might have indicated when they submitted their bid for</p> <p>2 the ad that Google should show this ad more to male</p> <p>3 users than to female users, and Google may have honored</p> <p>4 that request.</p> <p>5 A third possibility is that perhaps the</p> <p>6 Barrett Group indicated that the ad should be shown to</p> <p>7 high earners. In fact, in response from questions from</p> <p>8 the journalists at Pittsburgh Post-Gazette, the Barrett</p> <p>9 Group actually said that they were targeting users who</p> <p>10 are over the age of 45 and who earned more than \$100,000</p> <p>11 because they thought that would be an appropriate group</p> <p>12 to target for people who would want to go one level up</p> <p>13 and go after the 200K plus jobs.</p> <p>14 Now, it could be that these high earners are</p> <p>15 much more strongly correlated with the stronger</p> <p>16 correlation of the male gender than with the female</p> <p>17 gender, and Google may have inferred that and then</p> <p>18 decided that they should send more impressions of this</p> <p>19 ad to male users than to female users.</p> <p>20 Yet another possibility is that other</p> <p>21 advertisers might be targeting the female demographic</p> <p>22 more, and there is some evidence that female demographic</p> <p>23 is targeted more by advertisers, because they make more</p> <p>24 purchasing decisions, and those other ads may have come</p> <p>25 with higher bid amounts, which took up the slots for the</p>

145

1 female users, and the males just got these -- the ad  
 2 from this particular service because they were the  
 3 leftover, untargeted -- there were just more slots  
 4 available for the male users.  
 5 Yet another possibility, and this would be the  
 6 case of machine learning introducing discrimination, is  
 7 that Google's internal systems may have observed that  
 8 more male users are clicking on this particular ad than  
 9 female users, and since machine learning systems learn  
 10 from these kinds of observations, and they're trying to  
 11 optimize for the clickthrough rate, they may have served  
 12 -- started serving more impressions of this ad to the  
 13 male users.  
 14 So, all of these are hypothetical scenarios  
 15 because we don't have enough visibility into the system  
 16 to determine which of or if any of these situations --  
 17 possible explanations is the real explanation. But I  
 18 wanted to highlight this to explain the nuance of this  
 19 problem, that this is a very complicated problem, and if  
 20 you want to go towards making systems more accountable  
 21 in this space, then the researchers will need additional  
 22 access to the internals of the system.  
 23 So, being able to work not just from the  
 24 outside, like we have in this work, and Roxana will talk  
 25 about shortly in her work as well with the Sunlight

146

1 system, they have a similar model, but people on the  
 2 inside, who have more access might, if they are  
 3 interested in proactively testing their systems, that  
 4 additional step will be very crucial towards proactive  
 5 detection of violations, as well as of identifying  
 6 responsibility.  
 7 So, that is something that I would urge this  
 8 community to go towards, and it's an open call to  
 9 technology companies who work with researchers like us  
 10 to work on problems of this form that are socially  
 11 important.  
 12 So, let me stop here with the summary that  
 13 what this body of work, AdFisher, and a previous result  
 14 that introduces the methodology, brings rigorous  
 15 experimental design ideas to this research area, which  
 16 lets us discover causal effects, for example that it's  
 17 really the difference in gender that caused the  
 18 difference in high-paying job-related ads being  
 19 targeted, with statistical significance, so with  
 20 confidence that it's not just a fluke observation, but  
 21 it is really how the system is behaving.  
 22 And the third kind of contribution here is to  
 23 bring automation that allows us to discover these kinds  
 24 of effects at scale, and this combination was the first  
 25 in our work, and then the community has grown and

147

1 developed it in many different dimensions.  
 2 So, we found evidence of gender-based  
 3 discrimination that was one specific highlight, and the  
 4 other highlight is how browsing helped related websites  
 5 have a significant effect on targeting, in particular  
 6 how substance abuse -- browsing substance abuse websites  
 7 results in rehab ads being targeted.  
 8 And the two big open questions that I want us  
 9 to open up for discussion, and these are active areas of  
 10 research in this area, is how widespread is this  
 11 discrimination, and how do we go from here in assigning  
 12 responsibility. And as a corollary, I would like to  
 13 emphasize that additional access to the internals of the  
 14 systems, people with additional access to the internals  
 15 of the system, working with such people is going to be  
 16 highly crucial towards achieving these goals.  
 17 Thank you very much.  
 18 (Applause.)  
 19 MR. SALSBURG: Thank you, Anupam and Michael.  
 20 Now we're going to hear a presentation by  
 21 Roxana Geambasu of Columbia University titled Sunlight:  
 22 Fine-Grained Targeting Detection At Scale With  
 23 Statistical Confidence.  
 24 MS. GEAMBASU: Hello, everyone. I am very  
 25 happy to be here.

148

1 I will now tell you about some tools that we  
 2 are building at Columbia to increase the web's  
 3 transparency at large scale. To motivate our work, I'll  
 4 start with an example that shows just how opaque today's  
 5 web is. And you probably already know that Gmail uses  
 6 emails in order to target ads, but do you know how the  
 7 keywords or inferences drawn from these emails are being  
 8 used to target you, specifically? I'll test to see how  
 9 aware you are of how you're being targeted by showing  
 10 you some examples that we got from one experiment.  
 11 We created this Gmail account, and populated  
 12 it with a bunch of very simple single-topic emails, and  
 13 I'm showing here on the left-hand side, five of those  
 14 emails out of about 300 that we created. And on the --  
 15 you know, after that we retrieved ads that Gmail showed  
 16 in this account. And I'm showing here on the right-hand  
 17 side, ads, two ads out of about 20,000 that we got. So,  
 18 this was a pretty large-scale experiment.  
 19 And what I want to do is to challenge you guys  
 20 to tell me what each ad is targeting. So, for example,  
 21 what does ad one target? Which of the emails? What do  
 22 you think? Just quickly. Whatever comes to mind.  
 23 AUDIENCE MEMBER: Vacation.  
 24 MS. GEAMBASU: Vacation. Well, it actually  
 25 turns out that ad one targets the pregnancy-related

149	<p>1 email. You know, it's pretty hard to tell, right?</p> <p>2 Nothing in the ad really tells you anything about how</p> <p>3 it's actually targeted.</p> <p>4 What about ad two? It's about a hotel. What</p> <p>5 does this one target?</p> <p>6 AUDIENCE MEMBER: Homosexual.</p> <p>7 MS. GEAMBASU: You got it right. That's</p> <p>8 exactly right, the homosexuality-related email. Again,</p> <p>9 it's still pretty hard to tell. And it's not just about</p> <p>10 targeting of ads on Gmail that's hard to discern.</p> <p>11 Everything is obscure on the web.</p> <p>12 For example, you know, data brokers apparently</p> <p>13 are using -- you know, can tell when you're depressed</p> <p>14 and apparently sell this information. Or some credit</p> <p>15 companies, for example, are trying apparently now to use</p> <p>16 Facebook information in order to decide whether or not</p> <p>17 to give out a loan.</p> <p>18 You know, you may have heard of these things</p> <p>19 from the media, just like I did, but do you know that</p> <p>20 whether these things are actually happening, to what</p> <p>21 degree, and how those things affect you? I'll bet, you</p> <p>22 know, not -- you know, people don't know too much about</p> <p>23 these things.</p> <p>24 Welcome to the data-driven web. Many of the</p> <p>25 web services and third parties collect huge amounts of</p>	151	<p>1 know, on one hand so that on one hand we can increase</p> <p>2 users' awareness of what happens with their data online,</p> <p>3 and on the other hand, increase in power privacy</p> <p>4 watchdogs, such as the Federal Trade Commission, to</p> <p>5 monitor what all these services are doing with users'</p> <p>6 data and keep them accountable for their actions.</p> <p>7 And over the past several years, we've been</p> <p>8 building a number of these transparency infrastructures</p> <p>9 and we are continuing to do so now. And in this talk, I</p> <p>10 will tell you about just one of these, in the remaining</p> <p>11 time, just one of these infrastructures, the latest</p> <p>12 essentially public domain transparency infrastructure</p> <p>13 that we have built.</p> <p>14 Before I do that, I want to acknowledge my</p> <p>15 students and collaborators, without whom obviously I</p> <p>16 wouldn't be standing here, you know, telling you about</p> <p>17 these systems.</p> <p>18 So, what is Sunlight? Well, it's a generic</p> <p>19 and broadly applicable system that detects personal data</p> <p>20 use for the specific purpose of targeting and</p> <p>21 personalization. It detects which specific datum about</p> <p>22 a user, such as email searches, or visited websites are</p> <p>23 being used to target which service outputs, such as ads,</p> <p>24 recommendations or prices. The ads that I showed you at</p> <p>25 the beginning of the talk, their targeting, was</p>
150	<p>1 information about us, every location, every site, every</p> <p>2 site that we visit, every click that we make and so on.</p> <p>3 And they leverage all of this information for all sorts</p> <p>4 of purposes. Some in line with our interests. For</p> <p>5 example, we all love our Netflix recommendations or</p> <p>6 Pandora recommendations, but other uses may not be so</p> <p>7 beneficial for us. And the big problem is that we have</p> <p>8 absolutely no visibility into what happens with our data</p> <p>9 in this huge, complex web data ecosystem.</p> <p>10 Who has access to what data? For what</p> <p>11 purposes are they using it? Are the uses good or bad</p> <p>12 for us? You know, how do the uses affect us, really?</p> <p>13 And it's not just the end users that don't</p> <p>14 know how to answer these questions, but society as a</p> <p>15 whole has a hard time answering these questions. And I</p> <p>16 believe, you know, the FTC, you know, as well, from my</p> <p>17 communications with them a little bit. And that's very</p> <p>18 dangerous, because, you know, obscurity and lack of</p> <p>19 oversight can lead to abuses, either intentional or not.</p> <p>20 So, in my group at Columbia, we are developing</p> <p>21 these new kinds of tools which we call transparency</p> <p>22 infrastructures that shed light into this dark</p> <p>23 data-driven web. Our goal is to build really</p> <p>24 large-scale infrastructures that can go out there on the</p> <p>25 web and track the flow of information and reveal it, you</p>	152	<p>1 discovered by Sunlight.</p> <p>2 Sunlight has three unique properties compared</p> <p>3 to everything else that exists. It is precise,</p> <p>4 scalable, and very broadly applicable. We've already</p> <p>5 tried it with great success to reveal targeting of Gmail</p> <p>6 ads out in arbitrary websites, recommendations on Amazon</p> <p>7 and YouTube, and prices on various travel websites. Not</p> <p>8 all of these experiments are actually in open domain</p> <p>9 yet.</p> <p>10 And in all of these cases, Sunlight works with</p> <p>11 high precision, about 95 percent, as well as reasonable</p> <p>12 recall. How does it work? Well, the details are pretty</p> <p>13 complex, but at a high level, the idea is intuitive.</p> <p>14 Sunlight first started by correlating users' inputs,</p> <p>15 such as emails, with service outputs, like ads, by</p> <p>16 performing experiments on accounts with differentiated</p> <p>17 user inputs.</p> <p>18 We can actually make the link from correlation</p> <p>19 to causation if we control how those inputs are placed</p> <p>20 in the accounts. Let me show you an example quickly,</p> <p>21 just to illustrate this process.</p> <p>22 So, remember the ads that I showed you at the</p> <p>23 beginning of the talk? I'll show you how Sunlight might</p> <p>24 have detected their targeting, but let me first simplify</p> <p>25 the example a bit, so, you know, let's keep just three</p>

153

1 emails and one ad. And let's ditch the contents of the  
2 emails and ads.

3 So, what we have is a main account that  
4 consists of emails E1, E2 and E3. In these accounts is  
5 ad1. And what we want to do is to explain the targeting  
6 of ad1 on, you know, these -- one or a combination of  
7 these three emails.

8 What we'll do is three things: First, we will  
9 create a set of extra accounts, we call these shadow  
10 accounts, say three accounts, and populate them with  
11 different subsets of the emails. We do this randomly so  
12 that the placement of the emails into the accounts is  
13 random, is done randomly independent of any other  
14 variable.

15 Second, we collect ads from the shadow  
16 accounts and, you know, say, for example, in this  
17 example, that shadow accounts 2 and 3 observe ad1, but  
18 shadow account 1 doesn't. Third, we analyze these  
19 observations and yield the targeting prediction, and in  
20 this case, the most natural prediction that we would  
21 reach is that ad1 targets email 3 because the ad appears  
22 in all accounts with email 3, but never in accounts  
23 without email 3.

24 So, that's kind of how Sunlight works. And  
25 now there is an important distinction that I would like

154

1 to make, which is that the first two stages of this  
2 process populating shadow accounts with subsets of the  
3 emails and collecting ads from them, are  
4 service-specific, and pretty much in the mind in  
5 Sunlight, the frame of mind is pretty simple,  
6 simplistic, which adds to some browser automations.

7 The last stage, however, the analysis of these  
8 observations to yield the targeting prediction is  
9 intellectually challenging, and that's what Sunlight  
10 actually provides. Specifically, the example I showed  
11 you here is trivial. In reality, the scale is much  
12 larger, there are a lot more emails, you know, to  
13 consider, a lot more ads to explain, there is a lot more  
14 noise and so on.

15 So, all of these things make targeting  
16 prediction challenging, and Sunlight addresses these  
17 challenges by designing a rigorous methodology that  
18 leverages well-known methods from statistics to provide  
19 precise targeting predictions at scale.

20 And it does so, very importantly, and quite  
21 uniquely, in a service agnostic way so that we can reuse  
22 the analysis across many different services, like I said  
23 before.

24 So, let me now show you some of these  
25 challenges, just to exemplify the kinds of mechanisms

155

1 that we use to address them. Let's look at that simple  
2 example that we had with the three emails. Look at what  
3 we did. We used three shadow accounts in order to  
4 explain targeting on three emails. That's a pretty --  
5 that's a lot of accounts, shadow accounts that we needed  
6 to create.

7 What if we were trying to explain targeting on  
8 a more realistic user account with thousands of emails,  
9 and potentially other online activity, too, that  
10 compounds together with the emails to produce the ads.  
11 We would have needed to create, you know, would we have  
12 needed to create all combinations over a number of  
13 accounts that are equal to all combinations of these  
14 inputs. That is a scaling challenge, a huge scaling  
15 challenge that I think is tremendously important.

16 And, you know, it turns out, in fact, that we  
17 don't need as many extra accounts, we can get away with  
18 a lot fewer, only logarithmic number depending on the  
19 number of inputs that we are trying to explain targeting  
20 on, and my theoretician collaborator, Augustin  
21 Chaintreau, proved this aspect theoretically and we  
22 evaluated it experimentally.

23 And the intuition is that if we can assume  
24 that an ad targets only a small subset of the many  
25 inputs that we have in a main account, then we can

156

1 leverage sparsity properties, the same concept that are  
2 underlying compressed sensing, which say that you don't  
3 need a whole lot of observations in order to reconstruct  
4 accurately, you know, a sparse signal.

5 For those of you who are familiar with machine  
6 learning, I guess, we use, you know, that's what sparse  
7 regressions can also give, and that's what we use in  
8 Sunlight. However, these particular methods don't, you  
9 know, guarantee -- only guarantee logarithmic  
10 correctness, do not guarantee the correctness of any  
11 individual prediction. And what we want is a  
12 correctness assessment of individual targeting  
13 associations so that we can trust the results that we  
14 get from Sunlight.

15 And for that, what we do is we use hypothesis  
16 testing, just like in AdFisher, a well-known method that  
17 provides a quantification of the statistical  
18 significance of each prediction.

19 So, you know, Sunlight puts all of these  
20 things and other mechanisms together in a particular  
21 architecture that provides the unique aspect, you know,  
22 properties that I mentioned before, genericity and  
23 predictability, scalability and precision. I won't go  
24 into the details of this.

25 And instead, what I'll do in the, you know,

157

1 remaining two minutes, is I'll tell you, you know, how  
2 Sunlight can be used. Specifically, Sunlight is a  
3 transparency infrastructure which provides some valuable  
4 primitives for targeting prediction, and on top of it,  
5 we and others built transparency tools for studying  
6 specific services. And we've built a bunch of these  
7 tools, and it's actually extremely convenient to build  
8 on top of Sunlight.

9 I will tell you about just one of these tools  
10 that we have built, which we call the Gmail Ad  
11 Observatory. It's an online service that enables  
12 studies of targeting of Gmail ads on users' inboxes.  
13 Here's how it works: A researcher or journalist  
14 supplies a set of emails on which they want to detect  
15 targeting. The Gmail Ad Observatory uses the sort of  
16 Gmail accounts in order to send emails to a separate set  
17 of Gmail accounts that become then the shadow accounts  
18 from which we extract the observations, or collect the  
19 ads and infer the targeting.

20 The Gmail Ad Observatory then collects the ads  
21 periodically and supplies them to Sunlight to get the  
22 further targeting. And what we did, so this is kind of  
23 the tool that we built, and what we did was we used this  
24 tool to run a 33-day study of ad targeting in Gmail. A  
25 pretty large-scale study. We got overall about 20

158

1 million impressions of ads and, you know, about 20,000  
2 unique ads.

3 And what we found, we found a bunch of things,  
4 I'll show you just one result, which is a contradiction  
5 of one particular policy, or statement that Gmail makes  
6 in one of their FAQs. Specifically, what they say is  
7 that they do not target ads based on sensitive  
8 information, such as religion, sexual orientation,  
9 health, or sensitive financial categories. Well, guess  
10 what? We actually found examples, and a lot of  
11 examples, of ads that target each and every of these,  
12 you know, specific topics.

13 And I've already shown you, for example, the  
14 ad that targets the homosexual, you know, homosexuals.  
15 You know, let me show you another example from the  
16 health category specifically. You know, there are some  
17 senior-related, a lot, actually, of senior-assisted  
18 living ads that target Alzheimer's. Other ads, many ads  
19 actually that target Alzheimer's in general.

20 The results are an interesting ad that you can  
21 see there that targets the depression-related keywords,  
22 the "is he a cheater" ad for a cheating spouse or site,  
23 apparently. And there are a number of ads, as well, you  
24 know, in our example, that target the keyword cancer.  
25 I'm showing here just one of them. We found a number of

159

1 other ones.

2 MR. SALSBURG: You want to just take a  
3 sentence to wrap up.

4 MS. GEAMBASU: Yeah, that's right. So, to  
5 wrap it up, I've told you about our agenda of building  
6 generic and broadly applicable transparency tools which  
7 enable oversight at scale. These tools can be used to  
8 study targeting phenomena of various kinds, like ads  
9 targeting, for example, but not only, also price  
10 targeting, and I have actually a demo of that, if you  
11 guys would like to see it later.

12 Thank you.

13 MR. SALSBURG: Thank you, Roxana.  
14 (Applause.)

15 MR. SALSBURG: Our final big data and  
16 algorithm research presentation will be from Daniel Hsu  
17 of Columbia University. It's titled Discovering  
18 Unwarranted Associations in Data-Driven Applications  
19 with the FairTest Testing Toolkit.

20 MR. HSU: Thanks, Dan.

21 Okay, so I'm going to tell you about another  
22 tool that we've been developing at Columbia, and also at  
23 EPFL and at Cornell Tech. A lot of collaborators on  
24 this project.

25 So, I should preface this by saying that I am

160

1 sort of an outsider in this community. I mostly do  
2 research in machine learning and on the algorithms that  
3 are used by Google, by Yahoo, by Microsoft, for doing  
4 the data analysis, for maybe doing the targeting, and so  
5 this is kind of a, you know, has a different  
6 perspective. I'm going to give sort of a different  
7 perspective on this problem, and but, you know, you're  
8 all well aware of the kind of issues that come up with a  
9 lot of these data-driven applications. So, maybe you  
10 probably heard of this study that was done about  
11 detecting sort of differences in prices from Staples'  
12 online store that are based on where you live, and this  
13 turned out to have some kind of correlation with the  
14 income of potential customers, and this was sort of an  
15 interesting finding, but with sort of more interesting  
16 from our perspective is that this was an unintended  
17 consequence of the sort of pricing mechanism that  
18 Staples was using.

19 And, so, here's another example of this kind  
20 of data-driven application that may have some kind of  
21 unintended consequences. This was in the case of  
22 Google's image tagging application, where if you were to  
23 upload photos onto Google's social network services,  
24 Google would try to automatically tag your images with  
25 various things, like say there's a car here, here are

40 (Pages 157 to 160)

<p style="text-align: right;">161</p> <p>1 your friends, and there was very unfortunately an  2 incident where people found that some African American  3 users, their pictures were being tagged as gorillas, and  4 this was definitely not what Google was intending,  5 right? This is not something that, you know, they  6 wanted to happen.  7 So, you know, these are sort of problems that  8 arise when you are creating these kind of data-driven  9 applications. And what we want to argue in this work is  10 that these are, you know, these are bugs, and sort of  11 developers should be testing them, testing for these  12 kinds of bugs and trying to debug them, to correct these  13 issues, sort of in the same way that they would try to  14 correct or do debugging to find potential functionality  15 bugs, performance bugs and so on.  16 So, this is where our work comes in. We know  17 that, you know, this is not an easy -- this is not sort  18 of an easy problem to solve, these bugs are pretty  19 nefarious, they're pretty hard to detect. So, what  20 people might suggest is that, okay, you should take some  21 preventative measures, but these, we know, also have a  22 lot of limitations.  23 So, one thing you might suggest to do is,  24 okay, maybe we should just completely ignore certain  25 attributes about the data when we are designing these</p>	<p style="text-align: right;">163</p> <p>1 So, this is where our research comes in.  2 We've been developing this tool kit that we call  3 FairTest, and as we call it, a testing suite for  4 data-driven applications for developers to integrate  5 into their tool chain to try to, you know, check your  6 application, to do debugging, to run every time you  7 compile to make sure that the application is working as  8 they would want it to behave.  9 So, the way we kind of characterize it, or  10 caricature a data-driven application in a data-driven  11 application is somehow takes user data as inputs and  12 there is some kind of output that the application  13 provides, maybe the service prices, image tags, and  14 recommendations, and so on, looking for some kind of  15 function of these outputs.  16 And, so, maybe things like the user inputs,  17 might be like the locations of the users and their  18 profiles, whether they click on various things on the  19 website, and like we said, the applications outputs are  20 like the prices, the image tags.  21 So, FairTest comes in by something that you  22 could strap onto your development tool chain and look at  23 these kind of user inputs and the application outputs  24 and try to check for various kinds of unwarranted  25 association between the output and sort of protected</p>
<p style="text-align: right;">162</p> <p>1 data-driven applications so that we do not sort of  2 create these kind of unwarranted associations in the  3 service outputs. But we know this doesn't work, because  4 there are always sort of other attributes that may be  5 associated or correlated with the sort of sensitive  6 attributes like income level or race. This, indeed, is  7 what happened with the Staples pricing application where  8 location just happened to be sort of correlated with  9 income level. So, that might not work.  10 Another thing that you might try to do is to  11 apply some kinds of sanity checks like to see if there's  12 some kind of statistical parity in your outputs to make  13 sure that if you look at, you know, at race, you're not  14 sort of -- you're sort of at parity across the different  15 race attributes, but we know, again, this is not -- this  16 can be insufficient as well, just because there could  17 be, you know, sort of smaller subpopulations, you know,  18 with a particular attribute that end up having a strong  19 association with a service output.  20 So, these are really hard problems for  21 developers to solve. And, so, what we think we're  22 trying to argue here is that developers really do need  23 new tools to help them find these kinds of bugs. So,  24 detecting these kinds of unwarranted associations is  25 already a hard task for them to do.</p>	<p style="text-align: right;">164</p> <p>1 attributes that you wouldn't want to have some kind of  2 strong association there.  3 And, so, FairTest is a tool for automatically  4 doing this and it does this with some kind of data, and  5 the hope is that it will at the end produce some kind of  6 bug report that the developer will be able to look at.  7 So, what the developer would have to do is to  8 sort of specify which of the sort of user input are the  9 ones that are -- that we want to check for a strong  10 association with. These are what we call the protected  11 variables, protected attributes. These might be things  12 like the gender or the race of the user, and then there  13 are other many very likely, but many other attributes  14 that are used by the application, and these are things  15 that we're going to use to sort of try to define or to  16 search -- to define various kinds of contexts in which  17 there might be some kind of unwarranted association. And  18 then the last one I will talk about in a little bit.  19 So, the goal of FairTest, again, is to define  20 these kinds of context-specific associations between  21 some kind of protected attributes and the application  22 output, and then the bug reports is something that we'll  23 apply some statistics or machine learning in order to  24 produce something that the developer can understand in  25 terms of what does -- which kind of context, what kinds</p>

165

1 of associations were found by FairTest and to sort of  
2 rank them by the association trends or the statistical  
3 significance, so that is something that the developer  
4 can actually look at and understand.

5 So, let me say a little bit about how FairTest  
6 works. It's sort of, at its core, it's a machine  
7 learning algorithm or machine learning application, so  
8 FairTest itself is some kind of data-driven application.  
9 And the way that it works is that it starts by  
10 collecting or you start by providing it some kind of  
11 source of data. And here is where it's really important  
12 for the developer to really be -- to have some kind of  
13 source of data that is representative of a population of  
14 their user base, and this is where it's sort of  
15 difficult for maybe other parties to have access to  
16 this, but a developer presumably, you know, they're  
17 working -- they're like at Google or they're at  
18 Microsoft, so they have access to this kind of data  
19 already.

20 So, when they have this kind of data, they can  
21 really sort of check their application on the real user  
22 population to really discover the effects that have some  
23 meaning in terms of the actual users.

24 So, FairTest relies on this kind of data.  
25 And, so, what we'll do is something very similar to how

166

1 AdFisher and Sunlight operate, we will split this data  
2 into two parts, one we call the training data and the  
3 other part we call the test data. And we use the  
4 training data, so the part of the data set to sort of  
5 find these kinds of associations through some kind of  
6 clever machine learning algorithm. And then what if we  
7 find these kinds of sort of associations between  
8 protected attributes and physical application outputs,  
9 we'll use sort of remaining data, so sort of segregate  
10 it to actually validate these things and to measure  
11 their effect sizes and to check really are these things  
12 harming sort of a large segment of the population and is  
13 it very significant, and so on.

14 And this is where there's a lot of sort of  
15 technical machinery coming from machine learning. And  
16 then at the end, there are some, actually a lot of the  
17 work that's here is to make these kinds of findings sort  
18 of consumable by the application developer, so it's  
19 something that's interpretable and that they can  
20 actually use to help them maybe debug their application.

21 Let me give you an example. We actually  
22 applied this tool to a couple of sort of applications,  
23 some real applications that are sort of data-driven  
24 applications. So, one of them is the first one I wanted  
25 to tell you about is this sort of health care

167

1 application. This was actually sort of something that  
2 was produced by one of these machine learning contests  
3 or data science contests where some company, in this  
4 case it was Heritage Health Company, they ran this kind  
5 of competition where they tried to get -- you know, they  
6 provided some kind of data about patients going to  
7 hospitals and some sort of description of the patient  
8 records, you know, how many times they've been to the  
9 hospital before, you know, what were their symptoms,  
10 things like this. And the task was to use this kind of  
11 information to predict whether or not the or how many  
12 times the patient would come -- would visit the hospital  
13 in the next -- the following year. Sort of this kind of  
14 re-admission rate prediction.

15 So, what we did is we looked at the winning  
16 entry to this competition. It was a pretty good entry,  
17 sort of an application that was able to correctly  
18 predict with some pretty high accuracy, I think around  
19 85 percent accuracy, whether or not the patient would be  
20 re-admitted into the hospital the following year.

21 So, this was the data-driven application. It  
22 takes these kind of inputs, age, gender, number of times  
23 they've been to the hospital and so on, and then it  
24 tries to predict whether they will be re-admitted to the  
25 hospital.

168

1 So, what did we find by applying FairTest  
2 here? What we found was that there really are some  
3 specific contexts where there's an association between  
4 the age of the patient and how badly the predictions --  
5 how bad the predictions were. Sort of the rate of error  
6 rate or the size of the error in the prediction.

7 And, so, this was a -- this is sort of a  
8 contextual association that we discovered. It was not  
9 for the entire population, but sort of for some  
10 well-defined segment of the population. I think it was  
11 something like male patients who have been to the  
12 hospital at least or who have been to the ER at least  
13 like twice in the past year and so on.

14 But when we -- but within this subpopulation,  
15 there was a really strong effect, and a really strong  
16 association between age and the error in the prediction.

17 So, this is an interesting finding. We think  
18 that this is actually, you know, sort of important in a  
19 social sense, because this is something that could  
20 potentially really lead to actual harms, for instance,  
21 if this application was actually going to be used for  
22 insurance purposes, to do something to adjust your  
23 insurance premiums and so on.

24 So, these are associations that can really  
25 have some impact on the patients that they are -- or on

<p style="text-align: right;">169</p> <p>1 users that they are -- on users of the system.  2 I want to tell you about sort of another  3 application, this is not a real application, but it's  4 sort of a historical application, but it's something  5 that would illustrate sort of a different capability of  6 FairTest. So, this is a very well-known data set, sort  7 of the application you can think of as the graduate  8 school admissions application. What it does is it takes  9 people who apply to Berkeley graduate school and decides  10 whether to admit them or not.  11 So, this is a well-known data set from the  12 '70s. If you don't know what happened with this data  13 set, what happened was that they discovered out that  14 there was this kind of gender bias on the admission rate  15 at Berkeley, so men were being admitted at higher rates  16 than women. And, so, indeed, FairTest can be used to  17 discover this kind of association.  18 But what it can also do is it can try to  19 explain where this association comes from. And, indeed,  20 this is what this paper by Bickel, et al. In 1975  21 discovered was that, well, once you condition on which  22 department the applicant wanted to get into, then the  23 effect, either goes away or the impact maybe reverses,  24 that women in specific departments would be admitted at  25 higher rates than men.</p>	<p style="text-align: right;">171</p> <p>1 conscious and so on, and we think that they're just a  2 good way to start here.  3 Thank you.  4 (Applause.)  5 MR. SALSBURG: So, joining me on the stage now  6 are discussants James Cooper of George Mason University  7 Law School and Deirdre Mulligan of UC Berkeley.  8 So, we've just heard three presentations about  9 tools that are designed to shed some light on how data  10 is collected from consumers, how this results in them  11 receiving targeted ads, web content or result in  12 discrimination.  13 So, let me turn first to James and Deirdre.  14 What are the common themes you see running through these  15 three presentations?  16 MS. MULLIGAN: So, I teach at the School of  17 Information at Berkeley, and I spend -- one of the  18 departments in my -- one of the programs in which I  19 teach is a master's in data science, and we teach about  20 privacy, we teach about security, right, these are  21 people who are going to be doing data analytics, and one  22 of the areas where we've been lacking, both  23 methodologies and tools, is to deal with issues of  24 fairness, right? How do we think about the biases in  25 our data, how do we think about the biases in our</p>
<p style="text-align: right;">170</p> <p>1 So, this time what we wanted to do here is to  2 illustrate here how FairTest can be used to sort of help  3 a developer actually debug their system and try to  4 explain what was going on, what was going wrong in their  5 system. And maybe there's this other capability in  6 FairTest for doing this, we call it the sort of  7 providing some kind of explanatory variables, and this  8 was really aimed to this a real system or a real tool  9 for developers to use to debug their applications.  10 So, let me just make a few closing remarks.  11 So, we also applied FairTest in a couple of other  12 applications. You can read about it in our preprint,  13 which is available on the web. So, I already mentioned  14 this other feature of explanatory variables. There's  15 this other sort of big issue out there in data analysis,  16 which is that of adaptive data analysis, where you want  17 to be able to reuse a data set many times. This is  18 something that we're starting to look at and integrate  19 into FairTest, and this is sort of open source software  20 that can be used by developers right now.  21 So, just to sum up, really what we're trying  22 to advocate here is that we really need to empower  23 developers with sort of better statistical trainings,  24 better statistical tools in order to make these kind of  25 data-driven applications more fair, more sociably</p>	<p style="text-align: right;">172</p> <p>1 algorithms, and most importantly, I think what -- in  2 particular, and I'm kind of most deeply engaged with  3 Anupam and Michael's work, because we have some  4 collaborative work that we're doing, how do we think  5 about bias in systems where there are multiple inputs?  6 And, so, it's very difficult to track an output back to  7 a single actor's decisions.  8 And, so, as somebody who is working in that  9 sort of program, one of the things that I think is most  10 important about these tools is on the one hand, we have  11 our last presentation, FairTest, which is actually  12 trying to empower people who want to avoid, right -- all  13 algorithms have biases, all data -- if you design an  14 algorithm without a bias, it has no purpose in the  15 world, right? Let's be clear, right? It has a bias,  16 it's just that we want to avoid certain bad outcomes.  17 And the question about how we empower people  18 who are designing systems to proactively avoid those  19 outcomes is something that we need research on technical  20 systems that people have called for, oh, we need access  21 to the algorithm, we need access to the data as though  22 if they can look at it, they're going to understand it.  23 And that just isn't the case in many  24 instances, right? And, so, we actually need technical  25 systems, we need the use of statistical machine learning</p>

173

1 techniques to police machine learning systems.  
 2 And this is particularly important because I  
 3 think what all of them are highlighting and really  
 4 focusing on is not -- I mean, we're concerned about  
 5 intentional discrimination, but what I think many of us  
 6 are worried about exploding is disparate impact, right?  
 7 It's that nobody is intending for a bad thing to happen,  
 8 but because what machine learning enables, what makes it  
 9 different from what's gone before, is that the meaning  
 10 of information emerges, right?  
 11 And, so, it turns out that these three pieces  
 12 of data add up to some particular protected trait. And  
 13 as machine learning techniques continue to uncover the  
 14 way in which we have correlations that equate to these  
 15 different things, we're in this -- we have this ongoing  
 16 need to try to figure out proactively how to avoid those  
 17 sort of problematic correlations.  
 18 So, I think they're all working on this shared  
 19 problem from two different sides, right, that there's a  
 20 long history of testing and we think about  
 21 discrimination, housing discrimination, sending people  
 22 out in the world. And, so, I think the AdFisher and the  
 23 Sunlight are working on that side, right, can we test  
 24 from the outside, and then I think that Daniel's work is  
 25 really nice because it's saying, for the people who are

174

1 trying to do good, trying to avoid bad outcomes, can we  
 2 empower them with tools that are based on the same sorts  
 3 of statistical techniques that we need to police machine  
 4 learning. So, I think they're really powerful in that  
 5 way.  
 6 MR. SALSBURG: And, James, what do you see as  
 7 the common themes?  
 8 MR. COOPER: I would agree with what Deirdre  
 9 said. I mean, there are obviously, I think the common  
 10 themes are pretty self evident. I mean, the co-authors  
 11 are kind of back and forth on two papers, and all the  
 12 papers kind of describe algorithms that do various  
 13 similar work, and I think valuable work, as Deirdre  
 14 pointed out.  
 15 So, yeah, I mean, I don't really have much to  
 16 add beyond that.  
 17 MR. SALSBURG: So, Deirdre pointed out that in  
 18 the real world, there are lots of inputs. I mean,  
 19 consumer profile consists of it could be a million data  
 20 points, or more. How can your tools account for that?  
 21 When you're creating user profiles, is there any way to  
 22 know what would really be happening to a consumer?  
 23 MS. GEAMBASU: So, this is a real problem, a  
 24 very, very big problem. I would quote it as the biggest  
 25 problem in web transparency work, to date, in my

175

1 opinion, which is to actually emulate real users with  
 2 controlled experiments. All -- both of the -- both of  
 3 AdFisher and Sunlight rely on controlled experiments  
 4 with fake accounts that, you know, are assigned fake  
 5 input sets or inputs.  
 6 And that results in some targeting, we are  
 7 seeing, all of us, some targeting, but it's not  
 8 necessarily true that it's realistic kind of targeting  
 9 of the kind that real users would actually see.  
 10 We may be losing a lot of the targeting that  
 11 real users see. We may actually have targeting that  
 12 real users never see. And so on.  
 13 And I think that's a big, big problem. I  
 14 think we need research in designing tools that leverage  
 15 direct user -- data from real users in order to achieve  
 16 some of the goals that we have in our system,  
 17 transparency goals that we have in our systems.  
 18 That said, you know, I think, for example, I,  
 19 because I've been working so much and focused and been  
 20 invested so much in scalability, building scalable  
 21 systems that can take many inputs, but millions, not the  
 22 size that real users produce, certainly, you know, we've  
 23 been focusing on that. And Sunlight does scale pretty  
 24 well with respect to, you know, many, many -- trying  
 25 many, many inputs and discovering effects on many of

176

1 these inputs. But there are big limitations still even  
 2 there.  
 3 I also wanted to point out, because maybe the  
 4 audience didn't realize. So, FairTest and Sunlight were  
 5 actually, we're both collaborators on both, we just  
 6 split the talks so that we wouldn't have to create, you  
 7 know, to talk both about for each one of them.  
 8 MR. DATTA: Maybe one quick thing that I would  
 9 add here is there are two ways to go about getting  
 10 access to real data. So, one is to actually work with  
 11 the technology companies who have that data. And, so,  
 12 we have an ongoing collaboration now with Microsoft  
 13 Research where we are actually beginning to get started  
 14 with working with the internal data that they have about  
 15 their users.  
 16 The other way to do it, or at least one other  
 17 way to do it, is to try to get data from real users  
 18 through crowdsourcing. So, there is the recent  
 19 interesting paper from AT&T Research and collaborators  
 20 elsewhere, which tried to do that, so the way they do  
 21 their experiments is to just crowdsource it and collect  
 22 data from users about their browsing profiles, and then  
 23 compare it against the same user without the history.  
 24 Some amount of the history. And then see if there's a  
 25 differential treatment.

177	<p>1 So, that's beginning to get towards 2 experimental findings that have some amount of real user 3 data. 4 MR. SALSBURG: James, do you have a question 5 you want to throw out? 6 MR. COOPER: Well, sure. It's sort of a 7 question and a comment. I'm an academic, so, of course, 8 I'm going to spin my comment to say what I want to say 9 and then ask you. So, one of the issues, and I guess 10 this applies probably more to Michael and Anupam's 11 paper, but I think to all the papers, is, you know, if 12 we think about the transmission of your findings into 13 policy, I think one of the touchstones of policy, at 14 least in my view, should be harm. 15 So, I guess I think about your -- the finding 16 of the job search ad, different for men, different for 17 women, you know, and if you look at the statistics, 18 let's assume that the data is there and there's a 19 statistical difference and we can even say it's causal. 20 Digging down deeper, you know, what's the real-world 21 impact of that in the sense of, so, the click-through 22 rates are maybe, what, one out of a thousand, if you're 23 lucky, right? That's the average, right, one out of a 24 thousand? 25 So, let's say one out of a thousand people who</p>	179	<p>1 impact. I mean, you did detect -- so, you did find, you 2 know, a statistically significant difference between men 3 and women, but at the end of the day, before we get into 4 issues of harm, which I think should be a touchstone of 5 any policy, especially here at the FTC, you know, where 6 is -- do you need to find more? I mean, is there 7 actually some sort of evidence of harm here? 8 MR. TSCHANTZ: Well, there's the saying 9 amongst advertisers, which is I waste half of my budget, 10 I just wish I knew which half. So, I really don't think 11 anyone can look at any one ad and necessarily know what 12 its entire impact is, but we do know that advertisers -- 13 you don't see Coke ads on the TV because they expect you 14 to stop watching the TV and run out and buy a Coke, 15 right? 16 And these ads can be functioning in a similar 17 way. It's about creating an impact upon people that 18 lasts when they see something over and over again, or 19 don't see something over and over again. 20 So, we're concerned about the women not being 21 exposed to the encouragement to seek high-paying ads 22 just as much as we're concerned about whether any one 23 person clicks on that ad or not. 24 Now, I do think you raise an interesting point 25 about the fact that this firm putting up this ad, you</p>
178	<p>1 visit this website, they would click on that, and these 2 are people whose profiles have visited other job 3 searching websites. You know, so my point, or my 4 comment there would be to what extent -- they're not 5 going to be limited, this isn't really necessarily, hey, 6 I've gone to a thousand job websites, but now I've gone 7 to The Times of India and I'm just going to take a job, 8 I'm going to follow my career based on this ad that's 9 served to me, I think that's probably not likely. 10 And then, I visited both those websites, I'm 11 not sure, I'm sure you have, I don't know how many have, 12 but the ones at head-hunter website, I'm not sure, it's 13 got the nice banner, 200K plus, but it's a head-hunter. 14 I don't think -- I'm not saying it's -- I'm sure it's 15 legit, but I'm not suggesting the FTC look into it or 16 anything, but compared to the other one, where the women 17 were served more often, I think that was Jobs Near You. 18 And you go on that and the first page, 19 click-down menu, they're not blue collar jobs, they're 20 accountant, lawyer, bio. So, if you look at what would 21 be the real-world impact, if you could imagine the two 22 random people, the man and the woman. The woman who 23 says, well, I didn't see the head-hunter ad and so I'm 24 just going to go with jobs for me. 25 So, I look and I think about the real-world</p>	180	<p>1 know, I looked up its -- some customer reviews on it and 2 it didn't really have the highest customer reviews. So, 3 if we look at just the lack of perhaps women developing 4 a business relationship with them, then it might be 5 actually in their favor that they're not seeing this ad. 6 So, I don't know. You are correct, we can't 7 pinpoint and measure the exact amount of harm, but we do 8 know that men and women are being -- 9 MR. COOPER: Or any harm. I would just kind 10 of go that far. 11 MS. MULLIGAN: So, I think there are a few 12 things to highlight. One, there was another example 13 brought out about proximity to work, I don't remember 14 whose paper it was in. Was it in Daniel's? 15 MS. GEAMBASU: Proximity to the location of a 16 store. 17 MS. MULLIGAN: No, no, the proximity to work. 18 It may have been in the FTC's Big Data report that just 19 came out. And it's an example that's been used before, 20 if you were looking for a potential employee pool, 21 right, that you wanted to advertise to and you said, oh, 22 well people who live closer tend to be better employees, 23 and you might look and find out, well, that has a lot to 24 do with income or whatever, or it could be a proxy for 25 something else.</p>

181

1 And we do, when we're thinking about  
2 employment, equal access to not just employment  
3 opportunities, but also we think about the advertising  
4 of those employment opportunities as something where  
5 we're concerned about racial disparities and gender  
6 disparities and how we're making information about  
7 opportunities available, as a legal matter we're  
8 concerned about that. So, let me finish, hold on.

9 And, so, kind of setting aside this particular  
10 example, right, which we agree is problematic for many  
11 reasons, and I think, you know, one of the most  
12 interesting things that this particular example of the  
13 head-hunter ad brought out, which Anupam noted, is that  
14 the most likely, we think, or at least a highly likely  
15 reason that men were seeing this more than women is that  
16 people were willing to pay more to sell women -- to show  
17 women advertisements for, you know, hair care products  
18 and other things, right?

19 And the point being that if you were a company  
20 and you were trying to use this to make information  
21 available about employment opportunities, you don't have  
22 complete control over who sees them full stop. Right?  
23 And when we're thinking about anything that repliers --  
24 where you as an advertiser want to be attentive to who's  
25 getting access to your ads, because you're interested in

182

1 making sure that they are equally available to a  
2 population, define them whatever way you want, and you  
3 realize that there are other people whose bidding and  
4 decisions are interfering with your ability to know  
5 whether or not they're going equally to men and women,  
6 or they're going equally to people of different races,  
7 or whatever. You begin to say, wow, how do we think  
8 about causality, right, and how do we think about the  
9 relationship between bad outcomes and infrastructure,  
10 because it becomes an infrastructure issue.

11 Even if you are in the Staples example,  
12 Staples had access to their data, they were making  
13 decisions, they had access to lots of stuff, and they  
14 weren't seeking to have a particular bad outcome from  
15 your description, Daniel, yet they didn't do enough work  
16 or they didn't think through what was going to happen,  
17 right? So, again, it's about how do we create an  
18 infrastructure and tools.

19 MR. COOPER: Two things. To the extent -- my  
20 only point was using findings like this to inject into  
21 policy and the potential enforcement actions. You know,  
22 because that seems to be sort of the undercurrent in the  
23 papers, in at least two of them where, well, here's a  
24 Google privacy policy and, wait, my ad suggested there's  
25 tracking, which, you know, could lay the predicate.

183

1 So, my point is there seems to be a lack of  
2 harm. Now, in the Staples example, to say it's an  
3 unintended outcome, I think is completely unintended. I  
4 mean, that's just channel conflict mitigation. That's  
5 just the idea that I've got a brick-and-mortar store and  
6 I don't -- I mean, so that has nothing to do --

7 MS. MULLIGAN: Their intent wasn't to  
8 disempower people.

9 MR. COOPER: No, absolutely.

10 MS. MULLIGAN: And that's my point.

11 MR. COOPER: But I guess when you said they  
12 didn't intend the bad outcome, to them it's the correct  
13 outcome because it's the correct outcome based on that's  
14 the local pricing, I'm not going to undercut.

15 So, it has everything to do with competition  
16 and it has -- I mean, that has nothing to do with, wow  
17 -- you know, because there's actually -- you know, you  
18 think about, there's really no model that would set  
19 price discrimination and say, let's charge the poor  
20 people more than the rich people, and that's when -- you  
21 know, when I go to the movies and I hold up my George  
22 Mason ID, I try to cover the faculty part of it, right?  
23 And that's why, because they charge the students less,  
24 oh, you're faculty, sorry, you pay full price.

25 MR. DATTA: I have a brief, brief comment on

184

1 the question. So, for the job-related advertising  
2 example, I think this is where I was positioning this in  
3 that open problem of examining how widespread this  
4 phenomena is. This one particular ad is not enough for  
5 us to change how public policy works, but if -- and, you  
6 know, part of what Roxana is doing is building these  
7 infrastructures that allow examination of the entire  
8 Internet, possibly, a much more broader variety of  
9 sites, at scale, over many, many months, and you might  
10 -- if then she finds that there are many, many instances  
11 of these kinds of ads, maybe not this particular  
12 questionable ad, but from legitimate services that are  
13 showing up repeatedly in a differential treatment form,  
14 differential than the disparate impact, then the  
15 establishment of harm comment that you are saying is  
16 absolutely valid, that additional layer of analysis will  
17 not come from the kind of tools that we are building,  
18 that has to come from, you know, people like you and the  
19 regulatory agencies will look deeper, dig deeper into --  
20 dig deeper into is this really a legitimate disparate  
21 impact, additional harm consideration.

22 So, absolutely on board with you on that, in  
23 addition to the other comments.

24 MS. GEAMBASU: So, I just wanted to add  
25 something very, very brief, I completely agree with

185	<p>1 Anupam. What I wanted to note is that this research is  2 at the beginning. This kind of research into building  3 infrastructures that can, you know, tell what's  4 happening is at the beginning. And as a result, we know  5 very little.  6 We have a bunch of examples, right? That's  7 pretty much what we have. I have great hope for this  8 field, especially because more and more people are  9 coming into it, that we'll develop the kind of  10 infrastructures that we will need in order to actually  11 make impact on -- you know, in the legal domain. But  12 right now, you know, I think we know too little in order  13 to do that.  14 MR. DATTA: Short of having proof of existence  15 is useful as a starting point. We don't have evidence  16 that it's widespread. That's ongoing work.  17 MR. SALSBURG: I guess the good company that  18 wants to ensure it's not discriminating can use Daniel's  19 tool, and the others can get caught by the two other  20 tools.  21 MS. GEAMBASU: That's exactly the way we were  22 thinking and why we've been developing both from the  23 exterior, right, for the other thing, and tools for the  24 developers to actually help them, you know, figure out  25 what to do when the pressure is on from the exterior.</p>	187	<p>1 proceedings.)  2  3  4  5  6  7  8  9  10  11  12  13  14  15  16  17  18  19  20  21  22  23  24  25</p>
186	<p>1 MR. SALSBURG: So, we have 50 seconds, that  2 gives each of you about 10 seconds to do a final  3 thought.  4 MR. TSCHANTZ: Just to complete my thought,  5 you know, we've decided in employment men and women  6 should be treated the same. So, to me the fact that  7 they're not being treated the same is in and of itself a  8 harm. Maybe it's not to you, but that's my opinion.  9 MR. DATTA: So, I would say that we need a  10 complete accountability tool chain that goes from  11 detection to responsibility assignment to correction  12 mechanisms, and there is an emerging body of work on  13 each of these pieces of the puzzle. Our focus here has  14 primarily been on detection. There was a small amount  15 of explanations in the last talk, but there is a huge  16 set of open questions related to responsibility  17 assignment and corrective measures.  18 MS. GEAMBASU: It's okay.  19 MR. SALSBURG: Well, with that, we will wrap  20 up this session. So, thank you all so much. The  21 cafeteria will be open during this break, if you want to  22 go out and stand in a long, long line. So, we will be  23 back in 10 minutes.  24 (Applause.)  25 (Whereupon, there was a recess in the</p>	188	<p>1 SESSION 4  2 ECONOMICS OF PRIVACY AND SECURITY  3 MR. MORIARTY: Welcome back, everyone. My  4 name is Kevin Moriarty, I'm with the Federal Trade  5 Commission and this is session 4 on the economics of  6 privacy and security.  7 First we have Jens Grossklags from Penn State  8 University presenting An Empirical Study of Web  9 Vulnerability Discovery Ecosystems.  10 MR. GROSSKLAGS: So, welcome to the first of  11 two talks in this session that are actually about  12 security. This is joint work with Mingyi Zhao and Peng  13 Liu at the College of Information Science and Technology  14 at Penn State University.  15 So, my talk is about the topic of bug bounties  16 and vulnerability discovery that is mostly conducted by  17 external researchers that are often called white hats.  18 In 1995, the first bug bounty program was founded by  19 Netscape that invited external security researchers to  20 scrutinize its services. Since then, we had a number of  21 other company-sponsored programs emerging that were run  22 in an independent fashion. However, more recently we  23 actually observed the emergence of so-called bug bounty  24 platforms, and two of them are HackerOne and Wooyun,  25 which are the focus of our study.</p>

189

1 Wooyun was founded in 2010 and is mostly  
2 focused on the Chinese market. HackerOne operates in  
3 Europe and in the United States mostly and was founded  
4 in 2013.

5 So, the motivation for our study is to better  
6 understand how these bug vulnerability ecosystems  
7 actually operate and whether they make a significant  
8 contribution to web security. We also want to provide  
9 useful data for the policy heads, for example on the  
10 limits of vulnerability research and practice.

11 Our approach is to do an in-depth empirical  
12 study of these two ecosystems, and in our paper we take  
13 a very broad approach in the sense that we try to  
14 understand how organizations, white-hats, black-hats,  
15 the public interact on these third-party vulnerability  
16 platforms, but in the presentation, I will mostly focus  
17 on the perspective of companies and organizations.

18 So, the two programs that we look at have a  
19 couple of common aspects, mostly that's very popular, a  
20 lot of white-hats are interacting on them, and also a  
21 lot of vulnerability reports are made, but otherwise  
22 there are a couple of important differences. The first  
23 one is that HackerOne is "organization initiated" in the  
24 sense that these companies ask HackerOne to run a  
25 particular program for them versus on Weeyun, hackers

190

1 can actually submit -- any kind of hacker can submit any  
2 type of vulnerability about any website to the platform.

3 So, this is a very fundamental difference.  
4 There are some differences with respect to the bounties.  
5 Otherwise, also Wooyun is different in the sense that it  
6 doesn't delay full disclosure policies, so irrespective  
7 of the wishes of the company, after 45 days, the whole  
8 technical details of the discovered vulnerability will  
9 be communicated to the public.

10 So, there are some differences in the type of  
11 data we have about the platforms, so we cannot always  
12 directly contrast and compare the two, but what we can  
13 do is in five broad categories provide somewhat of a  
14 comparison on how these platforms actually operate.

15 The first one is participation. What we  
16 observe here is that on HackerOne, the number of public  
17 programs that are run is limited to about 100, and all  
18 of those are IT companies. In contrast, on Wooyun, we  
19 see a much broader portfolio of companies that are more  
20 or less coerced to participate on the platform. And  
21 interestingly, we see here a lot of organizations that  
22 typically are not known to run bounty programs by  
23 themselves, like government institutions, education  
24 institutions and also financial institutions.

25 So, the first takeaway that we have is that

191

1 the white-hat-initiated model allows for much broader  
2 participation and which may be good in the sense of web  
3 security. The more limited participation model or  
4 platform such as HackerOne, of course, raises then the  
5 question of how these platforms can actually encourage  
6 more companies to participate.

7 A second issue that we want to then explore is  
8 the quality of the submissions of what we observe here,  
9 in particular on the platform of Wooyun is that we have  
10 a very broad range of types of vulnerabilities that are  
11 submitted, and in 44 percent of these cases, these are  
12 actually classified as high-severity vulnerabilities.

13 On HackerOne, this is a little bit harder to  
14 determine from publicly available data; however, if you  
15 actually heard rumors of bounty amounts that are paid  
16 through the white-hat hackers, and also look into the  
17 policy statements, by combining these two data points,  
18 we can actually also then infer how many vulnerabilities  
19 are of high or medium severity, which is plotted on the  
20 slide.

21 So, here, we can also conclude that across  
22 these two programs, white-hats actually make significant  
23 contributions to the security of these websites by  
24 contributing high-severity vulnerabilities.

25 So, but more importantly speaking, the

192

1 white-hat model, white-hat-initiated model that is in  
2 Wooyun seems to harvest more of these vulnerabilities in  
3 an efficient fashion. Now, the question arises how well  
4 actually these different platforms and in particular the  
5 companies associated with them can actually respond to  
6 the submitted vulnerabilities. And here we see some  
7 interesting differences.

8 When we look at Wooyun, we can actually see  
9 that in particular, those very popular companies as  
10 measured by a measure of the Alexa rank, we see that  
11 most of them can actually adequately respond to the  
12 submitted vulnerabilities and handle them. In contrast,  
13 less popular and smaller websites very often are  
14 actually not capable to do so. So, in fact, about 25  
15 percent of the submitted vulnerabilities remain entirely  
16 unhandled by the organizations to which they are  
17 targeted.

18 On HackerOne, in contrast, since these are  
19 company-initiated programs, we see a very quick response  
20 time. Within four and a half hours, we see the first  
21 response to submitted vulnerabilities, and most of them  
22 are actually handled then within 30 days.

23 So, an interesting takeaway that isn't on this  
24 white-hat-initiated model on these platforms, we see  
25 that a lot of companies that are coerced to participate

193

1 are actually also not prepared, which is something that  
2 we have to take in consideration, versus -- and that, of  
3 course, then raises the question of balance. Well,  
4 should we actually coerce these companies to  
5 participate, is it a reasonable activity that we should  
6 be engaged in.

7 The next question that I'm approaching is, of  
8 course, of world interest, what impact do actually these  
9 kind of bounties have? Here is the first overview that  
10 we are seeing. So, what we are seeing here is a  
11 subsection or subassembly of companies participating on  
12 HackerOne. We see on the left side that some companies  
13 are actually not paying any bounties at all, versus  
14 others pay actually pretty substantial bounties for a  
15 submitted vulnerability.

16 On average, this doesn't really help us yet to  
17 determine what actually the really significant impact  
18 is, and for that purpose, we actually conducted a  
19 regression analysis in which the dependent variable is a  
20 number of vulnerabilities submitted, and the independent  
21 variables are the average bounty paid by a particular  
22 program, the popularity of the program, and a measure of  
23 the overall activity of the white-hats on the platform  
24 in the particular period.

25 So, what we are seeing here is first I want to

194

1 highlight the top part of the table, is that about a  
2 \$100 increase in the expected bounty pay towards  
3 white-hat researchers, we see about three more  
4 vulnerabilities reported to the programs. What we also  
5 see is that programs that are more popular are also  
6 receiving more vulnerability reports, and that, of  
7 course, has two factors.

8 One, more popular websites, of course, receive  
9 more attention, but often they are also more complex,  
10 they offer more services to the users, so they likely  
11 have a larger attack surface in the sense for white-hat  
12 researchers to find potential vulnerabilities.

13 So, the takeaway here is that white-hats do  
14 not necessarily always focus on monetary compensation.  
15 In fact, what we observed is that 20 percent of all  
16 contributions on HackerOne actually go to those services  
17 and programs that actually do not pay any bounties at  
18 all. So, pay nothing actually serves as a potentially  
19 viable approach.

20 In contrast, what we also observe is, well, a  
21 higher bounty amount at the end of the day is still  
22 associated also with a larger number of vulnerabilities  
23 that are submitted by the white-hat researchers.

24 So, which brings me then to the last question,  
25 the one about security improvements. So, what do we

195

1 actually get out of it? And in order to assess it,  
2 while we do not have an inside look into the  
3 organizations, we are using the trend of vulnerabilities  
4 submitted over time. So, the argument here is that if  
5 you have a declining trend of vulnerabilities,  
6 everything else, keeping moderately equal, then we would  
7 argue that perhaps at this particular website, the  
8 security is overall improving.

9 So, when we take a first look at the data and  
10 we see that it's actually rather spiky, so it's not  
11 immediately apparent by looking at these graphical  
12 depictions what kind of trends are emerging; however,  
13 one thing that we see in the top three graphs for  
14 HackerOne is that this seemingly initial spike, where  
15 once a program is opened, a lot of vulnerability  
16 researchers are submitting for vulnerabilities that they  
17 have stockpiled or that they have been essentially  
18 energized by the opening of the program to do  
19 immediately a lot of research that led to additional  
20 submissions.

21 Wooyun is a bit more noisy. So, in order to  
22 get a better understanding of how overall these trends  
23 shape out, we conducted a statistical test that's called  
24 the LaPlace Trend Test, and we focused here on programs  
25 that have a certain amount of minimum activity that were

196

1 running for at least four months, had at least 50  
2 vulnerability reports submitted to them. And what we  
3 see here is actually that two contrasting trends.

4 So, for HackerOne, we actually observed that  
5 over time for the majority of the programs, we see a  
6 decreasing trend of vulnerability reports. In contrast  
7 for Wooyun, which is a white-hat initiated, this coerced  
8 kind of company participation model, we see exactly the  
9 opposite. Mostly an increase in the vulnerabilities  
10 reported.

11 So, it would be reasonable that, and we could  
12 argue, well, despite monetary or perhaps because  
13 monetary incentives are in place, we actually see  
14 nonetheless there's fewer vulnerabilities on HackerOne.  
15 So, despite incentives, fewer vulnerabilities, we argue  
16 that this is indicative of actually improved web  
17 security practices at these participating companies. And  
18 keep in mind, again, that these participating companies  
19 are mostly IT companies in the case of the public  
20 HackerOne programs.

21 We also see this initial spike, which from a  
22 web security point of view might be really welcomed  
23 news, if, indeed, it's indicative that a lot of the  
24 stockpiled vulnerabilities are actually removed from the  
25 knowledge of white-hat and potentially black-hat

197

1 hackers.  
2 We see an opposing trend for Wooyun programs,  
3 and our interpretation of that is that, well, this  
4 likely has to do something with the lack of preparedness  
5 of these organizations when it comes to receiving these  
6 vulnerability reports.

7 So, for example, they may not have a  
8 well-developed, secure software developing life cycle,  
9 good integration between the security team and these  
10 external security developers, and many other factors  
11 might actually play a role here.

12 Which already brings me to the last point.  
13 So, we believe that it's instructive to conduct a really  
14 in-depth analysis of these programs to better understand  
15 what contribution they can actually make to its overall  
16 web security and practice. And it's definitely helpful  
17 that these two programs provided this as public data  
18 which we can study in detail. There are many more  
19 results which we actually have in the paper, in  
20 particular pertaining to how white-hats actually behave.

21 For example, we can showcase in our paper how  
22 white-hats learn from one another by investigating the  
23 reports of their fellow hackers. We can also study what  
24 kind of discovery participants have in place. For  
25 example, are they focusing on specific programs, or are

198

1 they applying the same kind of technique across very  
2 different websites.

3 So, there are a lot of interesting additional  
4 results, if you haven't already accumulated our papers,  
5 I encourage you to take a look at them.

6 In total, I believe that the jury is still out  
7 about which of these two participation models, the  
8 white-hat-initiated model or the company-initiated model  
9 are really giving us the best advantages.

10 On the first glance, it seems that the  
11 white-hat-initiated model really has strong benefits in  
12 terms of participation, so we see many more white-hats,  
13 many more organizations that are involved in these kind  
14 of ecosystems, but on the other hand, a lot of these  
15 participating organizations are not very well prepared  
16 when it comes to receiving these kind of vulnerability  
17 reports, and actually then improving also the security  
18 on their websites.

19 So, there are various kind of pros and cons  
20 that we can observe. One issue is clear is we can jump  
21 start or further engage in the discussion what kind of  
22 contributions overall these bounty programs make to the  
23 security of these websites. Our initial assessment is  
24 positive, but I think we can go into further detail  
25 during the discussion, and that brings me to the end of

199

1 my talk.

2 Thank you very much.  
3 (Applause.)

4 MR. MORIARTY: Thank you, Jens.

5 Next up we have Veronica Marotta and  
6 Alessandro Acquisti from the Carnegie Mellon University.

7 MR. ACQUISTI: Thank you and good afternoon.

8 This is joint work with Veronica, Kaifu Zhang and  
9 myself. If you know some of our previous work, you may  
10 know that often we use behavioral economics to try and  
11 understand how people make decisions about personal  
12 information. The study represented today is actually  
13 about traditional microeconomics, and it is about  
14 understanding the allocative and welfare impact of  
15 targeted advertising.

16 However, there is still a behavioral angle, at  
17 least in the motivations behind our work. In behavioral  
18 decision research, it is very well known that how you  
19 frame a certain problem influences the way people will  
20 think about this problem, and we make decisions about  
21 it.

22 And currently, we believe not only the age of  
23 the data, but also under a very powerful frame, the  
24 frame that personal data is the new oil, and we are all  
25 going to benefit, perhaps in equal parts, from the

200

1 collection and sharing and analysis of our personal  
2 information.

3 More specifically, there are a number of  
4 frames which are quite common in the public debate over  
5 privacy. For instance, personal information is the  
6 lifeblood of the Internet. So, the increasing -- the  
7 increasingly sophisticated collection of data is  
8 necessary for us to have free services online. Or loss  
9 of privacy is the price to pay to excel the benefits of  
10 the data, or sharing personal information is an economic  
11 win-win, which benefits equally data holders and data  
12 subjects.

13 Well, in our broader research agenda, we are  
14 interested in investigating all of these frames to see  
15 how actual empirical evidence there is supporting them  
16 or not supporting them.

17 The paper we are presenting today tackles the  
18 last frame, and more specifically, relates to the impact  
19 that targeted advertising has on the circles of  
20 different stakeholders. Consumers, advertising firms,  
21 and intermediaries, the ad networks. And Veronica will  
22 guide you through the model.

23 MS. MAROTTA: So, thank you, Alessandro.

24 So, the specific and integral question we are  
25 interested in addressing is to what extent the more and

201	<p>1 more precise information about consumers is due to  2 increasing in their welfare, what Alessandro just  3 referred to as the economic win-win, versus a change of  4 allocation of benefits among the different stakeholders,  5 including companies, consumers and online intermediaries  6 and platforms.</p> <p>7 Now, in order to address this question, we  8 rely on economic modeling to be the multi-stage  9 three-players model of online targeted advertising that  10 compare different scenarios that differ in the type and  11 the amount of consumers' information that is available  12 to the different players during the targeting process.</p> <p>13 Now, specifically differently from previous  14 work, we account for the important role played by the  15 intermediary in the advertising ecosystem, and we focus  16 on a specific mechanism of realtime bidding. Realtime  17 bidding is a technology introduced to facilitate the  18 location of program modeling advertisements online. Let  19 me explain quickly how it works.</p> <p>20 We have different players involved. On one  21 side, we have publishers, namely websites that wish to  22 sell advertisement space that is available on their  23 sites. On the other side, we have advertisers,  24 companies that wish to advertise their products online.  25 But those two players do not need to communicate</p>	203	<p>1 consumers directly. They need to rely on an  2 intermediary that facilitates the location of the  3 advertisements.</p> <p>4 We assume that the intermediary itself is a  5 profit-maximizing agent that receives a payment every  6 time he holds the auction for the advertisement's  7 location. Finally, consumers have product preferences,  8 but they need to know which seller is selling which  9 products. So, in this sense, advertising plays  10 informative role to consumers.</p> <p>11 Further, we assume that consumer can be  12 categorized by two categories of information: Horizontal  13 information, capturing consumers' preferences and  14 tastes; and vertical information, capturing differences  15 in purchase power.</p> <p>16 Now, these three players interact in our model  17 in this way: At a given point in time, a consumer is  18 online and he may be categorized by these two pieces of  19 information, horizontal and vertical. The ad exchange  20 receives the signal about a consumer, observes the  21 information, and holds an auction for the location of an  22 advertisement to that consumer.</p> <p>23 On the basis of the information that it  24 receives, advertisers form their bid. The auction is  25 run, the winner is determined, and it is allowed to show</p>
202	<p>1 directly, they can rely on the intermediary, the ad  2 exchange, that facilitates the location of  3 advertisements and the targeting process.</p> <p>4 So, the mechanism works as follows: When a  5 user arrives to a publisher's site, a signal is sent to  6 the ad exchange that is subsequently broadcasted along  7 with user data, maybe IP address, user cookies,  8 geolocation, to interested advertisers, and hold an  9 auction for the location of the advertisement.</p> <p>10 So, on the basis of the information that the  11 advertiser receives, they form a bid. So, how much are  12 you willing to pay to show an advertisement to that  13 user. And submit that bid to the ad exchange. Commonly,  14 the ad exchange uses second-price auctions. This means  15 that the highest bidder wins the auction, but he pays  16 the second-highest bid. So, once the bid -- the winner  17 is determined, it is allowed to show the advertisement  18 to the user.</p> <p>19 Now, on the basis of this mechanism, we built  20 a model that focuses on the interaction among three main  21 players: The advertisers, the intermediary and the  22 consumers. We assume that advertisers are  23 profit-maximizing agents, they want to advertise their  24 product to consumers that will like and therefore buy  25 their product. Nevertheless, they cannot target</p>	204	<p>1 the advertisement to the consumer. The consumer sees  2 the advertisement and makes his purchase decision.</p> <p>3 Now, it should be noted here that the outcome  4 of this process crucially depends on the information  5 that is available during the targeting process. So,  6 therefore, realize how the outcome for consumers,  7 advertisers and intermediary changes when different  8 types and amounts of consumers' information are  9 available.</p> <p>10 We considered specifically four cases. A case  11 where only the horizontal information is available, a  12 case where only the vertical information is available, a  13 case where both pieces of information are available, and  14 a benchmark case where no information about consumers is  15 available, so an extreme full privacy case.</p> <p>16 For each of these cases, we derive what's the  17 firm's best strategy, and therefore what's the firm's  18 profit; what's the intermediary payment received from  19 the location of the advertisements; and what's the  20 consumer's choice and surplus.</p> <p>21 Now, in the interest of time, I will not go  22 through the mathematics of the model, but I would like  23 to show you interesting results that we obtained by  24 simulating the model. So, what we do, we run  25 competition simulations to analyze how the outcome in</p>

205	<p>1 terms of consumer's surplus, intermediary's profit and 2 advertiser's profit changes when in the four different 3 informational scenarios.</p> <p>4 Let me start from the consumers. Now, the 5 graph that you see here, the X-axis captures how 6 heterogeneous consumers are in their preferences, while 7 the Y-axis captures how heterogeneous consumers are in 8 their purchase power.</p> <p>9 Now, important to note, low values means high 10 heterogeneity; high values means high homogeneity. Now, 11 the different colors corresponds to one of the different 12 informational scenarios that we considered.</p> <p>13 Specifically, each region captures under which scenarios 14 the consumers are better off.</p> <p>15 So, we have two predominant colors here. The 16 green region captures all the combinations of the model 17 parameters for which consumers are better off when only 18 the horizontal information is available during the 19 targeting process. So, what's the intuition there? In 20 their region, consumers are more heterogeneous in their 21 product preferences, therefore revealing the horizontal 22 information actually ensures that consumers see the 23 advertisements for the products they like the most. So, 24 there is a better matching between consumers and 25 companies.</p>	207	<p>1 intensifies the competition among the bidders. They may 2 tend to bid more aggressively.</p> <p>3 So, if we put together these two pictures, we 4 see that we have situations in which the interests of 5 these two players are actually aligned through the 6 yellow region, but there are also situations in which 7 they have contrasting interests. So, we may think a 8 situation of an intermediary that may have power over 9 the information about a consumer, and may decide to act 10 strategically, either by revealing the wrong type of 11 information, say green versus red region, or revealing 12 too much information when instead consumers would have 13 been better off with less information being revealed.</p> <p>14 Now, finally, we can use these simulations to 15 understand and analyze how the allocation of the 16 benefits among the different players changes under the 17 four scenarios, so we can construct a pie chart like the 18 one that we are seeing now for an information case, 19 where we see the percentage of the value generated with 20 auditing process that is captured by each player.</p> <p>21 So, we can have a pie chart for each scenario, 22 and what these pie charts show is actually part and very 23 similar to what we just discussed. Consumers in blue 24 tend to be better off either in the no informational 25 case or in the horizontal information case, while the</p>
206	<p>1 The yellow region, instead, captures all the 2 combinations of model parameters under which the 3 consumers are better off when none information about 4 them is revealed. So, in that region, consumers tend to 5 be more homogenous, so brands don't matter as much. So, 6 the targeting is not as available to consumers.</p> <p>7 Now, we can construct a similar graph for the 8 intermediary's profit. Again, we have two main regions. 9 The yellow region, again, is the combination of model 10 parameters for which the intermediary's profit now is 11 highest when none information is revealed about the 12 consumer. So, we said in that region consumers tend to 13 be more homogenous.</p> <p>14 So, what happens is that if advertiser had 15 that information, they will tend to bid lower to show 16 the advertisement, lower in the intermediary's profit, 17 but if the information is not revealed, then the 18 advertisers have to bid an expectation, so they may 19 overbid, increasing the intermediary's profit.</p> <p>20 The red region, instead, is the combination of 21 model parameters for which the intermediary's profit is 22 highest when the vertical information about the 23 consumers is available. In that region consumers are 24 more heterogenous, and so revealing actually the 25 vertical information during the targeting process</p>	208	<p>1 intermediary, in red, seems to capture a decent amount 2 of the benefits in all the cases, with the vertical 3 information one being by far the best case.</p> <p>4 For firms instead individually, it's always 5 better off to have at least some of the information 6 about the consumers with the complete information case 7 being in this case the best scenario.</p> <p>8 So, if you want to summarize those findings, 9 we find that consumers are generally better off either 10 when a specific type of information about them are 11 available, or, in general, when less information are 12 available. And that there exist situations where the 13 interest of the players, say the intermediary and 14 consumers, may be misaligned, and therefore a strategic 15 intermediary may choose to selectively share consumer 16 data in order to maximize its profits.</p> <p>17 So, I will leave Alessandro to some final 18 remarks.</p> <p>19 MR. ACQUISTI: Thank you.</p> <p>20 So, there are a number of extensions we are 21 planning or working on, probably the most important is 22 the empirical validation. In fact, if representatives 23 of ad networks are in the room or following from via 24 webcast, if you want to disprove or prove our results, 25 we would love to work with you.</p>

209

1 Now, going back to the broader picture from  
 2 where we started. On the left, you have the three  
 3 frames I started from, and I claim that they have  
 4 something in common, which is very little empirical  
 5 validation. So, I am not claiming that they're  
 6 necessarily wrong, I am claiming that we really don't  
 7 know how true they are.

8 So, on the right, instead, I have three broad  
 9 research questions that I believe are critical to really  
 10 understand to what extent they advertise the new oil and  
 11 to what extent the benefits of this new oil are  
 12 allocated, fairly or not, to the different stakeholders.

13 How is the surplus generated by data  
 14 allocated? If we use privacy technologies to find a nice  
 15 combination of protection of data and sharing of data,  
 16 are there some costs, and if so, who is suffering those  
 17 costs? Individual consumers, because they may get less  
 18 targeted advertising; society as a whole because maybe  
 19 the next medical researcher investigating cancer cannot  
 20 find a cure because he or she doesn't have enough data;  
 21 or it's just the issue of decreasing the rent exacted by  
 22 oligopolies that are in the industry. Very different  
 23 scenarios, and therefore also very different policy  
 24 conclusions.

25 And, finally, under what conditions consumers

210

1 still benefits from trades in their data and in what  
 2 conditions they do not, because I believe that the  
 3 answer is not binary, it's not always good or always  
 4 bad, it is very match context-dependent.

5 Now, this is a work in progress, in fact, this  
 6 work in our agenda. However, if you are interested in  
 7 the ground material in this area, and by this area I  
 8 mean the combined use of privacy, you can find on SSRN a  
 9 semifinal version of a paper that Curtis Taylor, Liad  
 10 Wagmanz and myself had accepted and it is forthcoming in  
 11 the Journal of Economic Literature. It's The Economics  
 12 of Privacy and we will leave with you this.

13 Thank you very much for your attention.  
 14 (Applause.)

15 MR. MORIARTY: Thank you, Veronica and  
 16 Alessandro. Next is Catherine Tucker from MIT to  
 17 present Privacy Protection, Personalized Medicine and  
 18 Genetic Testing.

19 MS. TUCKER: Okay, thank you very much for  
 20 having me. So, I'm Catherine Tucker and I am an  
 21 economist who studies the economic effects of different  
 22 types of privacy regulation using real-life data. And  
 23 what I'm going to be presenting today is joint work from  
 24 Amalia Miller where we investigate how different forms  
 25 of privacy protections affect consumer takeup of genetic

211

1 testing.

2 And because I know that a lot of you are here  
 3 to think about advertising and more mainstream issues, I  
 4 want to make a pitch for why this is interesting, before  
 5 you all go to your electronics.

6 The first reason, so why we think it's  
 7 interesting is that, first of all, this is a technology  
 8 with a huge upside, as I'll get to later. Secondly,  
 9 it's also a technology where I think even the most  
 10 cynical person about privacy would say there are  
 11 potential privacy consequences of this data being  
 12 created. Sometimes when you're thinking about targeted  
 13 advertising, it's hard to actually articulate the  
 14 privacy form, which is why we actually think about  
 15 health and financial examples, but when you think about  
 16 genetic data, it's not hard to come up with examples of  
 17 harm.

18 So, for example, I took a 23andMe test. I  
 19 will share with you, I found out, rather depressingly,  
 20 that I've got a few times more than average chance of  
 21 getting macular degeneration later in life, that means I  
 22 won't be able to see too well.

23 Now, the reason I feel confident announcing it  
 24 in this audience is because ultimately I have tenure at  
 25 MIT, I probably have the least potential consequences of

212

1 anyone in the world of releasing that kind of data  
 2 because I have a job and I have health insurance, but  
 3 there are potential -- you do not have to go far to  
 4 think of potential negative consequences of that data,  
 5 and as the previous presentation on genetic privacy  
 6 articulated, I think very well, there are also issues to  
 7 do with identifiability, the fact that this data is  
 8 persistent, and the fact that potentially this data has  
 9 spillovers to family members. So, it's really quite a  
 10 lot of privacy consequences.

11 The other reason I think this paper that we're  
 12 setting is useful is simply because there has been a lot  
 13 of experimentation about different kinds of regulation  
 14 which allows us to have more of a horse race than we  
 15 usually do when trying to evaluate how well privacy  
 16 protections work.

17 Now, I said there was an upside to this data,  
 18 I just talked about the downside to it being created,  
 19 but there's a huge upside. And the upside is the  
 20 promise of personalized medicine. And the typical  
 21 statement made in favor of the personalized medicine is  
 22 that for the average drug, based on your genetic makeup,  
 23 it won't work 25 percent of the time.

24 So, we can imagine if we actually have genetic  
 25 data, we will be able to identify effective drugs, and

<p style="text-align: right;">213</p> <p>1 save many drugs and save money at the same time.  2 Now, as well for these claims, I often find it  3 useful to sort of bring it to life with a very personal  4 example, which is the example of Angelina Jolie and how  5 genetic tests and the actions she took from it based on  6 it.  7 So, Angelina Jolie did genetic testing, she  8 found out that she unfortunately had a mutation in her  9 genes, which meant that she was likely to get both  10 breast and ovarian cancer; as a result had a double  11 mastectomy and a hysterectomy.  12 Now, this is obviously a strident and decisive  13 medical action, but in principle it's going to reduce  14 her chances of getting cancer by 70 percent. So, this  15 is the kind of data which actually leads to extreme  16 forms of action in a medical sense, but there's a huge  17 upside in health outcomes in terms of it being created.  18 Now, what we're going to do in the study is  19 look at state laws' experimentation with different types  20 of privacy regulation from 2000 to 2010. And what's  21 nice about this variation is you always worry in any  22 empirical study where the variation is coming from, why  23 are the states actually experimenting in this way as an  24 underlying reason.  25 From what we can see, it was pretty random,</p>	<p style="text-align: right;">215</p> <p>1 decisions to get to use genetic tests. We're lucky we  2 have a national sample that was done every five years in  3 the peer review study and they're going to be asking  4 30,000 people about whether or not they had a genetic  5 test in each sample.  6 Now, it's a great data set in one way, and  7 they focus on the decision to get a genetic test for  8 working out whether or not you have genetic  9 susceptibility towards breast and ovarian cancer. And  10 the reason I say this is a very interesting genetic test  11 is there is actually something you can do with this  12 information to save your life if you take the test. So,  13 potentially, this is a hugely valuable health -- piece  14 of health data to create.  15 Now, the negative is that this is a technology  16 in its early stages, and so as a result, we're only  17 seeing a little bit of takeup in our sample, about less  18 than one percent.  19 Now, what we're going to do in the paper is  20 use standard econometric techniques to relate the  21 decision of these people in our sample to go and get the  22 genetic test, to what the state privacy regime was like  23 in that particular year.  24 Now, I realize this is not an economist  25 audience, so what I want you to think of this is as the</p>
<p style="text-align: right;">214</p> <p>1 driven by individual state senators who got a bee in  2 their bonnet. And what we found also is nice, is that  3 they're experimenting with many different types of  4 privacy regulation, and we're going to bucket them in  5 the study into three buckets, which are informed  6 consent, regulating data use, and establishing property  7 rights.  8 And I want to -- in the past, what I've done  9 is I've said, well, you know, the great thing about this  10 is it actually emulates different countries' approaches  11 to doing privacy regulation. If you sort of think EU  12 and OECD approaches, more associative informed consent,  13 maybe the U.S., you can say we've thought about  14 restricting data use, and then there's sort of this  15 economist's dream of establishing property rights.  16 Now, I say that in the past, the reason I no  17 longer push it is I mentioned this once when I was  18 giving this talk in Paris, and this person from the  19 Ministry of Culture in France stood up and said, how  20 dare you say that, in France we regulate privacy in  21 every single way you could possibly imagine, so it's not  22 just one, but in general, what's nice about it is at  23 least we've got a horse race for different ways we might  24 think about regulating privacy.  25 Now, we're going to have data on people's</p>	<p style="text-align: right;">216</p> <p>1 statistical relationship that we do where we're  2 controlling for just about everything that you might  3 think of going on in the background. We're controlling  4 for the year, we're controlling for the state, we're  5 controlling for everything about the patient.  6 Now, if you like equations and subscripts, the  7 paper has got plenty of those, so I direct you there.  8 For now, though, for this audience, so what I  9 decided to do is to present the main results in a bar  10 chart, and the big punch line is, is that when we bucket  11 up our state regulations in this way, what we find is  12 that when you have informed consent, and that's informed  13 consent where we're telling people how the data is going  14 to be used, we get a reduction of a third or in terms of  15 how many people are taking a genetic test. Now, this is  16 a large proportion, but remember, these are quite small  17 numbers, so the baseline is small.  18 Now, when we have a usage restriction, that is  19 we say, oh, the state government says this data can't be  20 used to discriminate, say by employer, say by health  21 insurance companies, that really has no statistical  22 effect that we can measure. The thing which has this  23 big boost, or positive effect on the decision to get a  24 genetic test, is whether or not you actually give  25 individuals control over how that data will be used in</p>

217

1 the future.  
 2 Now, when you get results like this as an  
 3 economist, you're always going to worry, well, where are  
 4 they coming from and what's the explanation? So, one  
 5 explanation which worried me was maybe it's not about  
 6 the patients, maybe it's about hospitals and whether or  
 7 not they're offering the tests.  
 8 So, we went to the -- clicked more data to  
 9 test this, and we found that's not really the  
 10 explanation. It is the case that if you have these  
 11 consent laws, hospitals react negatively, that's not a  
 12 surprise. I've found that in the past. Basically it's  
 13 because you have to construct an entire parallel system.  
 14 However, what was important about this study  
 15 was we didn't find -- what we found was a negative  
 16 reaction by hospitals in terms of whether they offer  
 17 genetic tests to giving patients property rights.  
 18 Again, maybe not surprising, why would you set up a  
 19 genetic test in a facility of your hospital, probably to  
 20 do some research, and this is going to restrict your  
 21 ability to do research, but it suggests that the main  
 22 effect of having these individual controls positively  
 23 affecting outcomes is not driven by supply site, but  
 24 instead driven by patients.  
 25 Now, more proof of this is what, again, a

218

1 typical thing we would do in economics is we're always  
 2 going to worry about, well, you're saying this about  
 3 patients, but could there be another explanation of  
 4 something else going on in the state? We tested for  
 5 this by looking at alternative explanations.  
 6 One such test was we looked to see, well, if  
 7 we look at the decision to have an HIV test, which you  
 8 might say you think of as similarly sensitive to having  
 9 a genetic test, could we see any influence of the  
 10 genetic laws on that decision? We found absolutely  
 11 nothing, which suggests it's not driven by underlying  
 12 tastes or privacy in that state.  
 13 Similarly, we couldn't find genetic law  
 14 effects on flu shots, which suggests it's not driven by  
 15 tastes for preventative care.  
 16 So, what is really going on? I've pulled out  
 17 hospitals, I've pulled out disparate things from  
 18 spurious correlation to the state, and I think what  
 19 we're going to argue is that ultimately it makes sense  
 20 when you understand how this privacy information is  
 21 delivered.  
 22 Genetic testing is unusual in that you have  
 23 genetic counseling where you sit down with a genetic  
 24 counselor and you will discuss these privacy policies  
 25 for perhaps 20 minutes, as well as the positive and

219

1 negative consequences of taking a test. So, this is  
 2 very different from the typical online environment. We  
 3 know that consumers actually found out about some of  
 4 these laws.  
 5 The laws they don't find out about, though,  
 6 are the anti-discrimination laws. These are usually  
 7 part of the conversation, and I think that explains  
 8 really the lack of the fact that consumers just aren't  
 9 reassured because they don't find out about these laws  
 10 actually existing.  
 11 On the other hand, when you go through the  
 12 typical forms or process where someone is given informed  
 13 consent and told how the data could be used, but not  
 14 correspondingly given control, we are going to argue  
 15 that highlights a sense of powerlessness which perhaps  
 16 can explain some of the negative effect, whereas when  
 17 you restore control to the patient over how their data  
 18 might be used in the future, then you have reception  
 19 control which tends to be a positive effect, which might  
 20 encourage them going ahead with the test.  
 21 Now, we have some more material in the paper  
 22 where we try and prove that this really is about privacy  
 23 concerns in that we show that these effects are going to  
 24 be higher in situations where there's more likely to be  
 25 bad news if you have a genetic test, that is there's

220

1 reason to think you're going to have bad news from the  
 2 test; however, we also show there is absolutely no  
 3 effect if you've already got bad news. That is if  
 4 you've already had cancer, the bad news is out there  
 5 with your medical record, none of these privacy laws are  
 6 actually going to drive any of the effects.  
 7 I'm also going to show the effects are largest  
 8 for people who in their surveys took various privacy  
 9 protecting actions such as refusing to state income. So,  
 10 again, let's sort of draw it back to privacy rather than  
 11 someone else explaining my results.  
 12 So, let me just sum up what we found. So, I  
 13 want to emphasize, I think it's important for every  
 14 empirical study there's going to be limitations, and  
 15 certainly on this study, we do our best to try to make  
 16 it causal; however, you can always come up with a whole  
 17 bunch of explanations. We don't actually sit there in  
 18 that patient and genetic counselor room when they go  
 19 through the privacy policies, so we're speculating on  
 20 the mechanism based by reviewing the privacy policies  
 21 we've seen in different states, and the other biggest  
 22 advantage is there was a study in the early stage of  
 23 diffusion, and so this is going to be representative of  
 24 the individuals who embraced new technologies earlier.  
 25 Having said that, I do think there is

221

1 something to be learned, which is that where the states  
2 give more control over how private information is  
3 shared, we do see an increase in genetic testing, and we  
4 see this increase particularly for people who are  
5 worried that there may be bad news from the genetic  
6 test.

7 Now, we found that in general informed  
8 consent, that is giving people information about how  
9 their data will be used, without giving them  
10 corresponding control just deters patients, and both  
11 patients and hospitals from having genetic tests and  
12 offering genetic tests.

13 Lastly, we found that data usage policies have  
14 absolutely really little effect, and so it's either good  
15 or bad news, depending on how you look at it. I was  
16 quite positively encouraged because usually when I run a  
17 statistical relationship between a privacy regulation  
18 and economic outcomes, I find a negative effect, so I  
19 was pleased to find nothing bad.

20 On the other hand, these laws are designed to  
21 help people, and perhaps my research suggests that  
22 they're actually just not being publicized enough to  
23 reassure patients.

24 So, with that, I will say thank you very much,  
25 and I thank you again to the organizers for giving me

223

1 get firms to adopt these standards? We think they're  
2 underinvesting in security, so how do we get them to  
3 increase their security?

4 That's a great question. And, so, the story  
5 behind this empirical work is trying to understand the  
6 incentives of firms. Are there incentives? Do those  
7 incentives exist for them to adopt more security or an  
8 appropriate amount of security or a fair amount of  
9 security or an efficient amount of security? We're  
10 going to look at that.

11 The other motivation, for anyone who has had a  
12 conversation with me over the past few years, knows that  
13 I am keen on cyber insurance, and the kind of empirical  
14 work that cyber insurance can perform and how they can,  
15 at the end of the day, help assess the risk of firms.  
16 Really, that's what they're interested in, is  
17 understanding the variation of risk across their firms  
18 to price that. And the kind of de facto policy that  
19 they are creating now with these policies.

20 So, with those motivations, what I look at,  
21 the data set that I have comes from a company called  
22 Advisen, which is based in New York and provides loss  
23 and incident data to insurance companies. They have  
24 been creating the data set on cyber events for a number  
25 of years now, but traditionally they look at loss of

222

1 the chance to speak.

2 (Applause.)

3 MR. MORIARTY: Thank you, Catherine.

4 Next up is Sasha Romanosky of the RAND  
5 Corporation presenting Examining the Costs and Causes of  
6 Cyber Incidents.

7 MR. ROMANOSKY: This has been a long day,  
8 hasn't it? Thank you all for sticking around, and thank  
9 you to the FTC for hosting this. It's great to be here.

10 I'm Sasha Romanosky. I will present some  
11 empirical work related to cyber events, and I'll define  
12 those in a second, but I want to explain a bit of the  
13 motivation, or at least two motivations behind this  
14 work. One is you've probably heard of this executive  
15 order by the president a couple of years ago to try to  
16 improve critical infrastructure, and as part of that  
17 developed this beautiful framework for cyber security.  
18 So, if anyone has any questions about how to protect  
19 their systems, you can go to the standard and take a  
20 look and it will tell you everything you want to know.

21 The trouble with that is that it's a voluntary  
22 standard. It's not meant -- certainly not meant to be  
23 regulated in any kind of way, I think despite some of  
24 the criticisms people have had. And, so, the question  
25 then becomes how do you get firms to adopt? How do you

224

1 property, other kinds of general liability that firms  
2 will face, these are corporate data events related to  
3 loss and litigation.

4 Most of the data sets that you see up there  
5 relating to cyber events include 5,600 observations, we  
6 have a data set of 12,000. So, as far as I know, this  
7 is the largest data set of cyber events, data breaches  
8 and privacy violations, which is very nice because it  
9 allows us to do some analysis to try and understand  
10 better different kinds of patterns and the risks that we  
11 will talk about.

12 I am separating the different kinds of events.  
13 When I say a cyber event, they are generally broken into  
14 these categories as I'm defining them. There are  
15 certainly other ways of categorizing them, and that's  
16 perfectly reasonable. For the purpose of my talk here,  
17 I'm separating them into data breaches, we normally  
18 think about as an unauthorized disclosure of personal  
19 information; security incidents, attacks against a  
20 company for the purpose of causing harm to that company;  
21 for example, a denial of service, or a theft of  
22 intellectual property or an outage of a system; and  
23 privacy violations, so this is what I'm calling an  
24 unauthorized use or collection of personal information;  
25 and then other sorts of phishing and skimming attacks. I

225

1 think for this audience, we'll be mostly interested in  
 2 the data breaches and the privacy violations.  
 3 One differentiator between these, the data  
 4 breaches and the security incidents, what we might think  
 5 of as acts caused to the firm, so they are bearing and  
 6 they are suffering these attacks, as opposed to privacy  
 7 violations where the firm is engaging in some kind of  
 8 activity.  
 9 It's always useful to understand the  
 10 data-generating process to understand where the data are  
 11 coming from and what's included and what's not included.  
 12 And, so, to be clear, these data come from public  
 13 sources. There's no proprietary information. And  
 14 Advisen has a wonderful team of analysts that go out and  
 15 scour new sites, national and local news sites using  
 16 Freedom of Information Act requests, they find the  
 17 information using Lexis and West Law and other data  
 18 sources. So, they have amassed this wonderful  
 19 collection.  
 20 So, a cyber event will occur to a firm, a  
 21 condition on that it will be detected by the firm,  
 22 either by the firm, by a third party, by a consumer, by  
 23 law enforcement, somehow it's being observed by the  
 24 firm. We, of course, have no information about those  
 25 events which are not detected, that's just not in our

226

1 data set.  
 2 Given detection, it is disclosed to the  
 3 public. So certainly, of course, there is not always a  
 4 requirement for a firm to disclose an event. There are  
 5 exceptions, even with the breach notification laws. So,  
 6 we do not observe those that are not being disclosed.  
 7 Conditional on disclosure, we would hope it  
 8 would be reported within this data set, and of those  
 9 events that are recorded in the data set, some will lead  
 10 to a legal action, either private, public action, civil  
 11 or criminal.  
 12 To give you a sense of the overall totals, we  
 13 see that data breaches have, in fact, been increasing  
 14 over the past few years. So, these claims by others  
 15 that there are more breaches now than there were before  
 16 do seem to be true; however, we find that they are  
 17 increasing at a decreasing rate.  
 18 As opposed to security incidents, privacy  
 19 evaluations, and these phishing and skimming attacks,  
 20 which represent a much smaller proportion of the overall  
 21 incidents. So, we see the first takeaway from this is  
 22 that data breaches really represent the majority of  
 23 these events. Interestingly, security incidents seem to  
 24 be increasing at an increasing rate over the past few  
 25 years.

227

1 Now, as far as I know, there have been no  
 2 changes in regulation requiring disclosure, an increase  
 3 in disclosure of security incidents, and so conditioned  
 4 on the same level of reporting and detection. What this  
 5 that might suggest is that firms are being attacked more  
 6 now than they were before.  
 7 In regard to the insurance industry and trying  
 8 to understand the risk of their insureds, one way to  
 9 understand that is to look at analysis by industries. We  
 10 might want to understand what kinds of industries suffer  
 11 the greatest number of attacks or pose the greatest  
 12 risk. And, of course, there are many ways to think of  
 13 this. We could look at total number of events by  
 14 industry, but that gives us an incomplete picture. And,  
 15 so, we might look at the incident rate, proportion, the  
 16 percentage of firms within a given industry that  
 17 suffered the greatest number of attacks.  
 18 And then we could also look at lawsuits as  
 19 just an aggregate, and litigation rate. We could also  
 20 look at cost of events. I won't go through all of these  
 21 in the interest of time, but I'll show you these. So,  
 22 as a function of total incidents, the finance and  
 23 insurance industry suffer the greatest number of  
 24 incidents, followed by health care and government,  
 25 education and then manufacturing.

228

1 But as a function of incident rate, government  
 2 agencies, so these are states and local DMVs, law  
 3 enforcement, courts, suffer the greatest incident rate  
 4 followed by education.  
 5 Let me just skip through these. And then we  
 6 look at the legal actions. So, of the 1,700 or so legal  
 7 actions that we have recorded in this database, 300 or  
 8 so are criminal actions, and some filed in federal  
 9 court, some filed in state court, but really the bulk of  
 10 these legal actions are private actions brought --  
 11 private civil actions brought in federal court. And  
 12 these will be allegations of negligence, all sorts of  
 13 common law and statutory allegations.  
 14 So, negligence liability and strict liability  
 15 and breach of contract, unjust enrichment, a whole  
 16 smattering. From previous research, we found almost 80  
 17 -- over 80 unique causes of action brought by plaintiffs  
 18 in these suits.  
 19 When we look at the litigation, the total  
 20 number of litigation and litigation rate, we see the  
 21 privacy lawsuits have been increasing dramatically over  
 22 the years, whereas the data breaches have been held  
 23 steady. Now, these represent -- specifically these  
 24 privacy violations -- in regard to the lawsuits, the  
 25 privacy lawsuits, the allegations represent claims of

229	<p>1 typically unsolicited email or spam or faxing, 2 unsolicited telemarketing, or recording, either video or 3 audio recording.</p> <p>4 And overall, the litigation rate for data 5 breaches and security incidents has been decreasing over 6 the years, which confirms some of our previous work, and 7 so right now we're looking at a rate of about three or 8 four percent.</p> <p>9 What we also show here is that you'll notice 10 that the litigation rate for privacy violations is 11 really quite high, 95 percent, and I think this is 12 really just more of an artifact of the data. I think 13 while for the data breaches we can understand the sample 14 of breaches and identify which of those have been 15 litigated because of the breach notification laws, but 16 for privacy violations, we don't really have that same 17 denominator. We don't really understand the total 18 number of violations, and therefore the percentage of 19 which would lead to litigation. I think in our data 20 set, all we're really finding is that we're only 21 observing a privacy violation when a lawsuit is 22 occurring.</p> <p>23 Now, the next question, we're going to look at 24 some cost data, and so I will couch this by saying that 25 these are estimates of costs. They don't include --</p>	231	<p>1 that don't lose that much money.</p> <p>2 And, so, what we find here is that most 3 companies lose less than \$200,000. And, so, if you were 4 to ask me the question of how much does a data breach 5 cost, I would say less than \$200,000. And, so, this is 6 getting back with the incentives that firms may or may 7 not have investing in security and privacy protection 8 controls.</p> <p>9 The median cost is a little bit higher for 10 privacy violations, and that's still something we're 11 exploring to try and understand exactly why, but I think 12 the takeaway here is that this \$5 million, \$7 million 13 cost is overblown.</p> <p>14 We also wanted to look at repeat players. So, 15 this notion comes up quite a bit in different 16 conversations of what is the impact to firms that suffer 17 multiple kinds of events? Are they bearing higher 18 litigation rates, are they bearing a higher cost, how 19 often do they occur?</p> <p>20 What we find is that in our data set, almost 21 40 percent of firms are these so-called repeat players 22 suffering multiple events. And that's quite a bit 23 higher than I would have thought beforehand. I think 24 that's quite extraordinary, in fact.</p> <p>25 And, indeed, in the information and financial</p>
230	<p>1 certainly don't include lots of other information. They 2 are all firm-based, so typically first-party losses, 3 second- and third-party losses. So, all the costs that 4 a firm would incur because of a data breach that you 5 could imagine.</p> <p>6 So, the cost of notification, the cost of 7 forensics, the cost of repairing any IT systems. In 8 some cases, they represent a dollar figure loss, like a 9 financial loss. The third-party losses represent the 10 loss -- the cost of litigating. Litigating the lawsuit, 11 any kind of consumer redress, or financial sanctions 12 imposed by regulating agencies.</p> <p>13 So, given all these costs, the big question is 14 how much does the data breach cost. And, so, Poneman 15 has done a great -- have produced some great surveys 16 over the years trying to estimate these costs, and what 17 they come up with are typically figures of \$5 million, 18 \$7 million as the cost of the data breach.</p> <p>19 I might argue, though, that these -- this is 20 an improper measure because they're looking at the mean, 21 the statistical average, and so because of the variation 22 of the distribution of these costs, a median is a better 23 metric. So, not every data breach is a target of \$270 24 million and rising. Not every breach is Sony, not every 25 breach is JP Morgan or Home Depot. There are many firms</p>	232	<p>1 insurance sectors, almost 50 percent of them are repeat 2 players. I think that is quite interesting, also. The 3 figures here that I'm showing, \$9 and a half million 4 versus \$4 million are the mean, and what it's showing 5 you is that the cost for the repeat players is almost 6 twice, a little over twice than the nonrepeat players, 7 those that suffer just a single event. Now, the medians 8 are exactly -- showed exactly the same thing, that the 9 cost is higher for these repeat players.</p> <p>10 What I then also wanted to do is try to 11 understand, okay, well maybe \$200,000 is actually a lot 12 for these firms, so what does this represent as a 13 function of their revenue? So, what I did is went 14 through all of the data to try and understand what do 15 most companies lose as a function of their revenue and 16 then try and couch that relative to other kinds of 17 losses in different sorts of industries.</p> <p>18 So, we wanted to look at retail, there's 19 hospital, bad debt, global payment fraud. So, what you 20 could imagine is that Visa and MasterCard have a certain 21 tolerance for fraud, for bad debt, and that through 22 either an organic process or some calculations, they 23 have settled on some percentage. And these numbers come 24 from industry reports, showing 5.9 percent, 5.2 percent, 25 3.1 percent for fraud. Cyber events, less than half a</p>

233

1 percent. So, it's saying that cyber events cost less  
2 than half a percent of a firm's revenue, a great deal  
3 less than these other industries.

4 In addition to that, in other works by some  
5 colleagues, Lily Ablon at RAND, we conducted a survey  
6 using the American Life Panel, a great survey instrument  
7 that RAND has available to it to try and understand  
8 consumer sentiment towards breach notification. How do  
9 they feel and respond to firms getting these notices of  
10 a data breach?

11 And what we find is that for the most part,  
12 they're really quite content. They're really quite  
13 happy with responses that they're getting, with the  
14 timeliness, with the information presented in the  
15 notifications, and really have generally no concerns.  
16 There was a small percentage, though, of them that  
17 change firms, but by and large they are really quite  
18 happy.

19 So, consumer sentiment, if it is, in fact,  
20 high, coupled with a small cost to a firm because of  
21 these events, really may suggest that firms have very  
22 little incentive to change their practices. Thank you  
23 very much.

24 (Applause.)

25 MR. MORIARTY: Thank you, Sasha. And thank

234

1 you to everyone for those presentations. They were  
2 wonderful, and very varied.

3 So, I want to recap them briefly, but first I  
4 want to introduce Doug Smith who is from the Federal  
5 Trade Commission, and Siona Listokin from the George  
6 Mason University School of Policy, Government and  
7 International Affairs.

8 So, we had four very different presentations.  
9 Jens presented an evaluation of two bug bounty programs  
10 and offered conclusions about how they can be effective  
11 to identify, resolve and reduce vulnerabilities.

12 Veronica and Alessandro proposed an economic model for  
13 advertisers, platforms and consumers and concluded that  
14 the allocation of the benefits of sharing consumer  
15 information tends to benefit the platform and the  
16 advertiser. And if I'm wrong about any of these recaps,  
17 you can tell me in just a second.

18 Catherine presented an evaluation of the rate  
19 of genetic testing in states with privacy laws that fall  
20 into three different general categories, and concluded  
21 that states where redisclosure is restricted have the  
22 highest testing rates, and that states with informed  
23 consent decreases the rate of genetic testing.

24 And, finally, Sasha looked at one set of data  
25 and offered conclusions about the median cost of cyber

235

1 events, putting it around \$200,000 and less than what  
2 other studies have found about the cost of cyber events.

3 So, to start, I just want to turn it over to  
4 Siona to offer some thoughts and start the questions.

5 MS. LISTOKIN: So, Kevin had asked me to talk  
6 about themes in this panel, and I would note that the  
7 title of the panel is The Economics of Privacy and  
8 Security, and I think that's about as close as we will  
9 get to a theme. Lots of variation here. Papers covered  
10 some of the most important or touchstone topics in  
11 privacy, so health data, online advertising, and, of  
12 course, security.

13 I would also point out that the panel had a  
14 lot more focus on how firms respond to incentives and  
15 not just consumers. And, finally, a lot of talk, or the  
16 papers here really are a cross-section of stages of  
17 research design. So, if you think about economics of  
18 privacy, you've got a model that extends existing  
19 theory, descriptive papers using new data sets, and  
20 explanatory or causal papers.

21 So, my meta theme here is that the field of  
22 economics privacy is alive and well and quite robust,  
23 but that's going to be my question. So, extending  
24 Commissioner Brill's comments after lunch, and the  
25 conclusion at the end of Veronica and Alessandro's

236

1 paper, in this field, what's your wish list?

2 And this is for everyone. Where do you see  
3 the gaps in this literature, specifically as it would  
4 relate to policymakers and industry practice? So, not  
5 just advancing academic research. I'll start with  
6 Veronica and Alessandro, but I'm interested in  
7 everyone's thoughts.

8 MR. ACQUISTI: One comment, and I'll  
9 piggy-back on our last slides about the piece in jail,  
10 which contained a letter from SSRN. In doing that  
11 review the leaders from economics and privacy, we  
12 identified three ways of research. The field is not  
13 novel at all, actually it started in the late 1970s,  
14 early 1980s, with Chicago School scholars like Paulson  
15 and Stigler. So, there's a beautiful pedigree and also  
16 quite a bit of work starting back 40 years or so.

17 However, only at the time there no models,  
18 like the late '70s, early '80s, no models or  
19 microeconomics in the field of privacy, it was more  
20 about using economic concepts, such as asymmetric  
21 information, models of that, and apply them to privacy.  
22 What we have now is lots of careful modern work, and  
23 what we start to see in maybe the last five years, 10  
24 years, in terms of the work of folks like Catherine  
25 Tucker and others, it's beautiful empirical work.

<p style="text-align: right;">237</p> <p>1 So, in terms of my wish list is to see even 2 more empirical work, and in order to have more empirical 3 work, sometimes we need data from the industry. So, if 4 the industry is serious and believes really that data is 5 the new oil, and that more transparency is good for 6 everyone, then we should address the problem of 7 information asymmetry that Serge was referring to as one 8 of the questionable problems we had in the previous 9 panel, which is we really want more data from the 10 industry regarding exactly what they do with the 11 information they collect.</p> <p>12 So that even if people, the end users, may 13 disregard their privacy policies, they may not care 14 about what companies are doing, researchers can actually 15 study the data and then come out and aggregate it and 16 understand what is really happening and then come up 17 with maybe policy recommendations.</p> <p>18 So, my wish list is more empirical work and 19 more transparency from the industry side.</p> <p>20 MS. LISTOKIN: Go ahead.</p> <p>21 MR. ROMANOSKY: I mean, I would echo that, 22 right? I think there has been a lot of time spent doing 23 what a colleague would refer to as admiring the problem, 24 and I think that's useful, and I think that's good, and 25 I think that only gets us so far.</p>	<p style="text-align: right;">239</p> <p>1 affect wage levels.</p> <p>2 However, if I'm a policymaker making really 3 important decisions about whether to regulate privacy or 4 data, I'm instead relying on just a handful of studies 5 in potentially none generalizable spheres. So, really 6 it's almost personnel and numerosity.</p> <p>7 MR. GROSSKLAGS: I want to add something. On 8 my wish list is perhaps a better understanding of the 9 long-term consequences of both the loss of privacy and 10 potential security compromises, and some work that 11 Alessandro and I have done goes in that direction to 12 understand how people perceive privacy decision-making 13 over time, but what we could not assess in a robust 14 manner is what are actually the potential losses that we 15 may face down the road. And I think this is a very 16 critical issue when it comes to genetic privacy, but 17 also to consumer privacy.</p> <p>18 A similar issue also rises in the context of 19 security, where actually the most interesting things 20 might happen in the context of what we do not observe. 21 Right? So, you saw it in Sasha's chart, we could only 22 analyze the data that was detected. So, what about all 23 the security breaches that we do not observe and that we 24 know nothing about?</p> <p>25 Similar with respect to my presentation, there</p>
<p style="text-align: right;">238</p> <p>1 I like empirical work because it speaks to 2 evidence for something. It gets us past normatives and 3 values and what should there be, and it really speaks, 4 it really helps answer the effect of, you know, what 5 will be the effect of A on B. And certainly, you know, 6 the causal inference is the gold standard. So, in order 7 to do that, you know, the point is exactly true, you 8 know, we need the data, right?</p> <p>9 And sometimes that takes us being very 10 creative on finding it in clever ways like the previous 11 panel, the researchers did themselves, coming up with 12 these experiments, which I think is beautiful. And 13 sometimes it takes paying for it which, you know, is 14 okay, too. But certainly I think we need the empirical 15 work.</p> <p>16 So, I would echo everything Alessandro had to 17 say, especially in the wonderful accented way that he 18 said it.</p> <p>19 MS. TUCKER: Well, I'll just add to the 20 accents. So I, you know, unsurprisingly, I agree for the 21 need for empirical work. What always strikes me is if 22 I'm a policymaker trying to decide if I want a minimum 23 wage, or what the level of the minimum wage should be, I 24 could draw on hundreds of economic studies that have 25 measured in hundreds of different ways how minimum wages</p>	<p style="text-align: right;">240</p> <p>1 is the behavioral white-hats, which we can now analyze 2 in a reasonable fashion, even though this was one of the 3 first works doing that, but what we do not observe is 4 the behavior of black-hats, and there we still have a 5 lot of work to be done in terms of investigating them 6 and getting maybe qualitative data, but also tying 7 together data sets such as Sasha's with, for example, 8 analysis that we have done to kind of be able to infer 9 where vulnerabilities have been known by the black-hat 10 community that had not been discovered by the 11 white-hats.</p> <p>12 MR. ACQUISTI: May I add something? Jens has 13 really said something really important about long-term 14 effects, and here is the dilemma that is a field day 15 that privacy faces. In my belief, the most interesting 16 implications of data sharing and data protection are 17 long-term and indirect. But generally, as economists, 18 we can publish and do rigorous work when we have 19 shorter, indirect effects. It's very, very difficult to 20 do studies and find causal links over long spans of time 21 when there could be a data breach now which only has an 22 effect seven years later, and you are not going to 23 satisfy reviewers in a rigorous type journal with 24 analysts who try to find those kind of effects.</p> <p>25 So, this data is far afield. I don't think</p>

241

1 there is any simple methodological solution to that.

2 MS. LISTOKIN: Thanks.

3 MR. SMITH: I guess it's my turn. I have a  
4 question for the group, and I'm actually going to ask  
5 one of Catherine first. Catherine, so, you know, what  
6 your research showed is that different laws have  
7 different effects on consumers' choices in this  
8 particular context of sort of genetic privacy.

9 So, I was curious, sort of how you think this  
10 research -- what implications it has for other areas of  
11 privacy and data security?

12 MS. TUCKER: Okay. So, what was nice about  
13 this setting is it allowed us to have more of a horse  
14 race, where we had the same thing we were trying to  
15 explain in lots of different privacy regimes. Now, the  
16 extent of -- the reason I find it useful or reassuring  
17 is it helps me believe some of the other research I have  
18 done in other areas, which have been more case by case.

19 So, some of the research I have done, for  
20 example, in targeted advertising, which a lot of people  
21 have talked about today, is emphasize the negative  
22 effects of informed consent, but also positive effects  
23 from improving consumer perceptions of control. But I  
24 was always nervous because those were two very separate  
25 studies, different at different times, different

242

1 spheres, even different countries, and so I found it  
2 reassuring to actually use this horse race to make me  
3 think, well, perhaps there is something more  
4 generalizable we can say about the effectiveness of  
5 different privacy regimes.

6 MR. SMITH: Thanks. And then, the question I  
7 have for the group, is actually just a little bit of a  
8 follow-up on one of the things Siona pointed out, which  
9 is that you guys are looking a lot at how firms' choices  
10 have in this arena, so what is your -- what do these  
11 papers, and research in general, suggest about what the  
12 private sector is getting right? What is it getting  
13 wrong? You know, what can this improve on our  
14 understanding of what kind of market failures might be  
15 most concerned about in this area?

16 Why don't we start at this end I guess.

17 MR. GROSSKLAGS: What is the private sector  
18 getting right? I think one -- one observation that also  
19 Alessandro and I have made over the time is that we see  
20 a lot of entities, private entities entering the market  
21 with privacy-enhancing offers, but not really picked up  
22 in the marketplace to a sufficient degree. And, well,  
23 the good news is that we do see these offers, we see a  
24 lot of technological solutions that are eventually  
25 picked up by startups, but what we see less is an

243

1 adoption by the big players because of a lack of  
2 incentives.

3 Targeted marketing or advertisement is just  
4 too enticing to give it up in exchange for a more  
5 privacy-friendly practical solution. So, that's a  
6 fundamental conundrum that we are presented with that is  
7 very hard to sidestep.

8 Nevertheless, I think it's very important that  
9 we see these new offers in the marketplace, and I hope  
10 more of them are actually picked up and practiced.

11 MS. LISTOKIN: What are they getting right?

12 MR. ACQUISTI: Well, getting back to Jens'  
13 point about offers in the marketplace, one reason for  
14 optimism is I think the sense of privacy enhancing  
15 technologies, PETs. So, almost every time I'm invited  
16 here to the FTC I end my talk talking about PETs because  
17 I really strongly believe that technology is not just  
18 the problem, it can be the solution. Privacy  
19 technologists do not stop altogether the flow of data,  
20 but rather modulate, right? They are sharing the  
21 protection.

22 So, the reason for what privacy firms can  
23 actually make, this may be wishful thinking, but may be  
24 provocative in deploying PETs, anticipating otherwise  
25 very little regulatory integration, so that they can

244

1 still do much of what they are doing now, but in a more  
2 privacy-preserving manner.

3 Now, truth to be told, some of these  
4 technologies are still in its -- in their infancy. For  
5 instance, metamorphic encryption are still very  
6 promising, but we still don't know how efficient and  
7 practical it would be, but the promising is enough for  
8 the moment, and I do believe that we could in this race  
9 for privacy, we can actually have the cake and eat it,  
10 too, because of these technologies.

11 MR. ROMANOSKY: In terms of what are firms  
12 getting right, God, that's such a good question, and I  
13 wish I had a better answer than the one I'm about to  
14 give. I think -- so, I think what we can rely on is  
15 that firms will -- firms will -- firms will operate  
16 based on incentives. And, of course, the goal then is  
17 to tweak the incentives such that they become aligned  
18 for all of the players, right? So, that's not new.

19 And what that means is that, you know, look,  
20 if privacy really is a big deal, then consumers should  
21 really act like it's a big deal, and if -- and only  
22 until they do will firms have incentive to take it  
23 seriously. So, I guess I need to -- I guess I would say  
24 that consumers should take it seriously, and act like  
25 it, and then firms will take it seriously.

245

1 Now, if there are -- if there are market  
2 failures for which consumers can't -- you know, can't  
3 impose any kind of effect on the firm, then that's  
4 where, you know, that's where regulation or policy or  
5 FTC actions can come into play.

6 Go ahead.

7 MS. TUCKER: No, I just wanted to build on  
8 that, because I think what I often see in the discussion  
9 is this underlying assumption that it's never in firms'  
10 interest to regulate on privacy. And so that -- and  
11 therefore, government has to intervene. But I think  
12 there are instances that we see in research where there  
13 are incentives for firms to actually improve privacy  
14 protections for consumers.

15 For example, the provision of user-centric  
16 controls, and so I sort of see that as a beam of light  
17 in a rather cynical world.

18 MR. ROMANOSKY: Yeah, and I think, I mean, it  
19 does touch on the world of information disclosure and  
20 choice and notice, and poor choice and notice. You  
21 know? Poor choice, over the past five, six years, has  
22 taken a beating, hasn't it? But it's relied on this  
23 notion that, you know, firms don't behave the right way,  
24 consumers don't behave the right way because they don't  
25 have the right information, and only if we could give

246

1 them the right information would they make the proper  
2 choices.

3 I'm just not sure that's true. At least let  
4 me say it this way, that maybe firms, at least in my  
5 case, with the data, that maybe firms do have the right  
6 information, maybe they are aware of all of the risks  
7 that using and collecting the data have, and that maybe  
8 they are making rational choices. And for them,  
9 investing a certain amount, which we may think is  
10 underinvesting, isn't the proper amount, but maybe it is  
11 actually the right amount as far as they're concerned.

12 MR. GROSSKLAGS: I just want to also add that  
13 this panel was also about security, and I think one  
14 thing that firms do right is participating in bug bounty  
15 programs, and really taking serious efforts in hardening  
16 their web security, but also other security aspects. And  
17 I think they're still quite a step away from anything  
18 approaching full security, but I think having a  
19 multi-dimensional security program, including bug bounty  
20 programs, is definitely a step in the right direction.

21 MR. MORIARTY: Jens, on a related point, I  
22 wanted to ask you, there was a notorious blog post by  
23 the chief information officer of Oracle where she sort  
24 of denigrated the value of bug bounty programs, and  
25 basically the analysis was, look, it's very expensive to

247

1 go through all these bug reports, it very rarely yields  
2 useful information. Your study does show that there are  
3 benefits to participation, but I think the question that  
4 she was raising is, are the benefits of participation  
5 greater than the benefit of just using that same money  
6 to pay another engineer to evaluate internally the  
7 controls in your software?

8 MR. GROSSKLAGS: So, bug bounty programs are  
9 certainly not the first security measure that any kind  
10 of company should implement; however, as you saw in one  
11 of my early slides, actually very mature companies from  
12 a security point of view were the ones running their own  
13 bug bounty programs, like Facebook and Google and so on.  
14 So, from that perspective, it was worth their while.

15 And certainly one of the main selling points  
16 is that it provides a different perspective, in addition  
17 to running software security tools, having internal  
18 security researchers, in the sense that white-hat  
19 researchers have perhaps somewhat more of a view like a  
20 black-hatted organization, they are more creative, there  
21 are protocols in places where other security researchers  
22 would not look, and this is certainly a big selling  
23 point to inch the security of your website even a couple  
24 of steps further.

25 Also, I think there's a lot of criticism about

248

1 these bad ratios between the reports and the data that  
2 is actually then useful, and I think when you actually  
3 look very closely at it, a lot has to do with the matter  
4 of duplicate reports. And, well, I mean, this is  
5 actually white-hat researchers doing their job. If the  
6 reports have not yet been disclosed, then, well, they  
7 will report oftentimes the same kind of security  
8 weaknesses to the particular entity, and, well, taking  
9 this into account, then actually the error rate is not  
10 that high.

11 Last point here is that here, actually the  
12 involvement of bug bounty platforms can really have a  
13 positive impact, because they can introduce measures  
14 such as reputation mechanisms, adding security walls and  
15 so on that actually then also instill some part of  
16 competition between the white-hat community participants  
17 so that they are more inclined to actually provide  
18 high-quality data to the participating companies.

19 MR. MORIARTY: All right, we have 20 seconds  
20 left. So, Siona, do you have any final thoughts?

21 MS. MAROTTA: May I add something?

22 MR. MORIARTY: Yeah, Veronica, please.

23 MS. MAROTTA: Yeah, I wanted to clarify there  
24 are a number of findings where we don't find that  
25 intermediary is always bad, but sometimes it does do the

249	<p>1 right things for the consumers, so there are, like, 2 policy in this case is more nuanced. So there are cases 3 in which the intermediary is -- the interest of the 4 intermediary is aligned with the consumers, but there 5 are cases which, instead, its incentives may be 6 contrasting with those consumers. 7 MR. MORIARTY: And your paper is not currently 8 up on our website, but I believe that we will have it up 9 following this presentation so people can, if they want 10 more information about your findings, they can look at 11 it there. 12 Well, thank you all for participating in this 13 session. We really appreciate it. Thank you. 14 (Applause.) 15 (Whereupon, there was a recess in the 16 proceedings.) 17 18 19 20 21 22 23 24 25</p>	251	<p>1 enforce security protocols, which we use in computers 2 and phones. This makes it pretty difficult, first of 3 all, to implement security protocols on these devices, 4 but apart from that, a big issue is that the current 5 smart phone model works like this: 6 Your devices inside the home send all your 7 information to the cloud, to a particular server. In 8 fact, if you have two devices in the home and they want 9 to talk to each other, currently they talk to the cloud, 10 and the information will get back to the home, and 11 something will happen in the home then. 12 So, what we have is a pretty bad combination. 13 You have hardware which is incapable, and you have 14 information which is always being sent to the cloud. 15 So, this combination results in potential privacy 16 problems. 17 Now IoT devices which are sending network 18 traffic without security protocols may end up leaking 19 some information about the user. They may end up 20 leaking information about what device is being used 21 inside the home, and they may also end up leaking 22 information about whether the user is home or what he is 23 currently up to. 24 So, in a sense, what I am saying is anybody 25 sitting on your network port may be able to find out</p>
250	<p>1 SESSION 5 2 SECURITY AND USABILITY 3 MR. ALVA: Our last panel of the day will look 4 at issues around security and usability as it relates to 5 privacy. So, I would like to welcome our first 6 presenter, Sarthak Grover. He is a Ph.D. student at 7 Princeton. 8 MR. GROVER: Thanks, Aaron. 9 Hi, everyone. I'm Sarthak, and I'll be 10 presenting our work on The Internet of Unpatched Things. 11 So, the main aim here is to basically look at the 12 current state of devices. We basically ended up 13 studying network traffic from a bunch of smart devices 14 which are really popular, and we want to talk about how 15 these devices may potentially leak user information. 16 My aim is to encourage you to think of how we 17 can improve policies to stop this potential leak of 18 information. So, how is the smart home or the IoT 19 environment very different from the conventional mobile 20 or computer environment? The problem here is that we 21 have a lot of manufacturers, and we have small startups 22 coming up with their own devices. They may be hiding 23 device programmers. 24 Apart from that, these devices have low 25 memories. They might not have capable hardware to</p>	252	<p>1 what you are doing inside your home, and this is a big 2 problem. So, what our aim is right now is to basically 3 take up a few devices in our case study and study what 4 kind of personal information or user activity 5 information they leak to the cloud. 6 So, what we did was we basically bought some 7 popular devices. We went to Amazon.com, we searched for 8 some very popular home network devices which people are 9 currently using in their smart homes, and we ordered 10 them. What I am going to show you is results for 11 network traffic analysis for five particular devices: A 12 camera, a photo frame, a hub, an Ubi smart speaker, 13 which is like an Amazon Echo, basically, and a Nest 14 Thermostat. 15 So, what we are interested in right now is 16 what kind of information these common devices leak to 17 the network. And the first device I pick up is the 18 digital photo frame by PixStar. So, what we found out 19 was that all traffic from this photo frame is sending 20 clear text. There is absolutely no encryption happening, 21 all right? 22 The cool thing is that this device can 23 actually talk to your Facebook or RSS feed, so it's 24 downloading photographs in the clear; and also, whatever 25 action you take on this device -- for example, you press</p>

253

1 a button, say you press the play radio button -- that  
2 will actually go in a clear HTTP packet which somebody,  
3 again, on the network can read.

4 So, if there is somebody sitting outside on  
5 the network, like somebody in the ISP or a malicious  
6 passive listener, they can see what you're doing through  
7 the photo frame. Apart from that, it's also capable of  
8 downloading radio streams, again, in the clear.

9 So, an example of what kind of information we  
10 see, so these are snapshots from Wireshark basically,  
11 and what we saw was that your email, which you  
12 configured your account with, is actually being sent in  
13 clear text. What this means is that this photo frame is  
14 potentially leaking account data, and anybody on the  
15 network port can actually have a look at this email.

16 Secondly, if you press a button on this photo  
17 frame, say you a press the "List Contacts" button or the  
18 "Radio" button, anybody, again, on the network IoT can  
19 have a look at what you currently pressed. So, somebody  
20 on the ISP can go, like, this person is currently  
21 listening to the radio from his digital photo frame,  
22 though I don't know why you would listen to the radio  
23 from the photo frame anyway. So, basically what I mean  
24 to say is that you can find out about the user's  
25 activity, as well as some other information, just by

254

1 looking at the network information.

2 The second device we picked up was a Sharx  
3 security camera. It's a pretty common camera which is  
4 used for security monitoring in homes. It has, like,  
5 motion detection. What we saw was that all the traffic,  
6 again, was being sent in clear text.

7 Now, this security camera actually requires a  
8 login. So, if you want to view the stream, you are  
9 supposed to enter a password, but that doesn't mean the  
10 stream itself is encrypted. In fact, anybody sitting on  
11 the network can still have a look at where the stream is  
12 going and what the stream is.

13 Also, if you go to the web interface and you  
14 press a button, whatever you did will still go in an  
15 HTTP GET packet, again unencrypted. So, videos are  
16 being sent as JPEG frames. Also, if you have pressed  
17 the FTP button, then all your data is being uploaded to  
18 the FTP, again in the clear.

19 And this is an example of what things look  
20 like. So, the FTP is actually using some pretty random  
21 ports, so you can't really rely on the network to secure  
22 you, again, because these are nonstandard ports which  
23 are being used by the device. And things -- like, this  
24 is basically private data which is being uploaded.

25 The third device we ended up looking at was

255

1 the Ubi. So, this I think is like a precursor to the  
2 Amazon Echo. Basically, it's a small voicebox which you  
3 can talk to, interface with other devices. For example,  
4 we had this Ubi interface with the Nest Thermostat in  
5 our houses.

6 So, what we saw was that all voice to text  
7 first of all gets converted -- all voice you talk to  
8 through the Ubi will get converted to text on the device  
9 itself, and then text is sent in clear, again, to a  
10 server outside. The server here was the Ubi.com.

11 Apart from that, the Ubi also has certain  
12 sensors, for example, light sensors and temperature  
13 sensors, which are still sending readings in the clear.  
14 And the interesting thing over here is when we  
15 interfaced this device with the Nest, it used encryption  
16 and spoke over HTTPS, but when it was talking to its own  
17 server, it was using HTTP, and everything was in clear.

18 So, clearly, this device actually has the  
19 capability of enforcing security, but somehow, the  
20 policy, whatever policy they came up with, they did not  
21 enforce encryption for their own device streams. Only  
22 when they're talking to the Google API, they enforce  
23 this encryption.

24 So this is an example which shows how sensor  
25 readings were available. Now, these sensor readings can

256

1 leak information about whether the light is on in the  
2 room or not. In a sense, somebody on the network, who's  
3 on the path, can know whether there's a user inside the  
4 room or not based on the luminosity value.

5 Furthermore, when you were chatting with the  
6 device, all the text was converted to clear text and  
7 then sent to the network. So, here you can see an  
8 example of what the chats looked like when I monitored  
9 them on the laptop gateway.

10 The next device we looked at was the Nest  
11 Thermostat. Now, we're actually coming to the more  
12 secure devices and the big ones, too. The Nest  
13 Thermostat from Google actually was pretty secure. All  
14 the information was over port 443, basically using  
15 encryption and HTTPS.

16 Now, what we also found out was that some of  
17 the updates incoming were in the clear, and we weren't  
18 sure why, so we contacted Nest about this; found out it  
19 was a bug, and they fixed it.

20 So, here is an example of what we found  
21 initially. Outgoing traffic was secure, but incoming  
22 traffic, some of the updates were not secure. They were  
23 in the clear text, they had some information regarding  
24 the location, and when we told Nest about it, they  
25 thanked us, and they fixed it.

257

1 All right. And the last device which I'm  
2 going to talk about is the Smarthings Hub by Samsung.  
3 Again, a pretty popular hub from a pretty big company.  
4 The good thing was almost all the traffic coming out of  
5 this device or going into the device was totally secure  
6 over DNS. There was no clear text or port 80 traffic at  
7 all, and the flows were all to Amazon AWS instance.  
8 But the interesting thing is, even though this  
9 device is in itself secure -- and, in fact, I see this  
10 as the model of future IoT devices, which are completely  
11 secure, there is still some background information, like  
12 three or five packets every 10 seconds, going to  
13 smarthings.com, which can somehow let you fingerprint  
14 the device.  
15 The good thing is that the Smarthings is a  
16 hub. Basically, what that means is that you have other  
17 sensors attached to Smarthings over some other  
18 protocols, like ZigBee or bluetooth or Z-Wave, and you  
19 don't have a direct view of the sensors, so Smarthings  
20 itself makes all the information coming out of the house  
21 secure and then sends it out. But a person sitting at  
22 the ISP level can still find out that, you know, you  
23 have a Smarthings Hub inside the home.  
24 So, this brings us to my conclusion and some  
25 implications on the policy. Basically, I don't want to

258

1 sound pessimistic or dramatic, but that's what the  
2 heading is, "Be Afraid!" We know it's very difficult to  
3 enforce security standards on smart devices. Inherently,  
4 I mean, there are multiple manufacturers. There are only  
5 a few big ones, but a long tail of small ones. Smart  
6 devices come up on Kickstarter, and people buy them.  
7 It's difficult to ensure that they all follow the same  
8 standard.  
9 These devices are also sometimes very low  
10 capability. They don't even have a way to implement DNS  
11 on the packets they're sending out, and they also end up  
12 using nonstandard ports and protocols. But the good  
13 thing is that we are trying to make an effort. For  
14 example, I found this handout outside regarding  
15 "Building Security in the Internet of Things," and  
16 that's good, because it means we're trying to enforce  
17 security at the building block level itself. So, maybe  
18 the new devices which come out would have security  
19 inherent in them.  
20 The second thing is, okay, so we fixed devices  
21 which are coming up now. What about devices which are  
22 already present? How do we get people to patch them up  
23 or fix them? So, for example, we want to encourage  
24 people to look for bugs, and one way would be bug  
25 bounties, but as we've seen in previous talks, you know,

259

1 bug bounties may work for the big guys, but the IoT  
2 domain has a lot of small manufacturers coming up, and  
3 we don't really know if bug bounties will work for that,  
4 and we don't know if the device will be popular enough  
5 to have users which actually look for vulnerabilities in  
6 them.  
7 So, the main point is, how do we enforce such  
8 kind of things? Like, who is responsible here? Will  
9 the Government try to enforce bug bounty programs or is  
10 it the manufacturer which goes, if you find a bug, we  
11 will give you money?  
12 And lastly, who pays for this patching in the  
13 update part? If this is using your network, is the user  
14 responsible for anything which goes wrong or the ISP or  
15 is it the manufacturers?  
16 So, I want to end with some of the work which  
17 we are currently up to right now. So, we've talked  
18 about how we can improve future devices in terms of  
19 their security and privacy policies. We've talked about  
20 how we can improve current devices by trying to find  
21 bugs in them and vulnerabilities in them.  
22 The approach we are taking right now is how to  
23 improve security and privacy policy on the network.  
24 Basically, we are trying to offload policy to the  
25 network layer. For example, in case of a smart home,

260

1 all our information is going to go through a gateway  
2 which is inside the house. This gateway might be  
3 provided to us by the ISP or it might be our own, but  
4 maybe there are parts of security that we can implement  
5 at the gateway itself. Maybe we can tell the gateway to  
6 enforce certain standards regarding the network  
7 protocols which are being used by devices or, at the  
8 very least, this gateway would inform our user that,  
9 hey, there's something wrong with your devices or this  
10 device is not using the right security standards.  
11 So, what we are looking at currently is can we  
12 offload device security to a gateway or the network  
13 layer? And secondly, how much information about the  
14 user behavior is actually leaked to outside the home  
15 network?  
16 All right, thank you.  
17 (Applause.)  
18 MR. ALVA: Thank you.  
19 Next we will have Professor Vitaly from  
20 Cornell University and Cornell Tech.  
21 MR. SHMATIKOV: Hi. So, I am Vitaly, and I'll  
22 be talking about mobile advertising today. Mobile  
23 advertising is pretty big these days. If you look at  
24 modern app stores, you find that a significant fraction  
25 of apps are free to the user, and the way they make

261

1 their money is by incorporating advertising.

2 So, it seems like a very reasonable question  
3 to ask, what information about the user is actually  
4 available to advertisers? That is, if an advertiser  
5 submits an ad through a mobile ad network and that ad  
6 gets shown on a user's phone, what can an advertiser  
7 find out about the user of the phone on which the ad is  
8 being shown?

9 So, that seems like an interesting question  
10 for which, apparently so far, there hasn't been a good  
11 answer. Very few people have investigated this, so this  
12 is what we decided to investigate in this project, to  
13 look at this. But in order to understand this, we first  
14 need to understand how mobile advertising actually works  
15 from a software perspective. So, it requires a little  
16 bit of reverse engineering of how mobile software  
17 actually shows ads to users, how it actually works.

18 Mobile advertising is a little bit similar to  
19 web advertising with one crucial difference. So, in web  
20 advertising, you typically have a web browser and the  
21 web browser is just showing an ad. That has been  
22 studied a lot, and even today, we have heard a lot of  
23 talks and conversation about web advertising.

24 In mobile advertising, things are a little  
25 different because there is something in the middle;

262

1 namely, there is an app library. So, the way mobile  
2 advertising works is that apps that are supported by  
3 advertising, they typically include a little piece of  
4 code called an ad library, and it's that piece of code  
5 that's actually showing ads. It's not the app itself.  
6 It's the ad library inside the code.

7 And it's actually very common for modern apps  
8 to incorporate multiple advertising libraries because  
9 they make more money that way. So, maybe between a  
10 third to half of all apps that are ad-supported actually  
11 include multiple advertising libraries for multiple  
12 providers that are being used to show ads to users.

13 So, the question I'm asking, just to repeat  
14 it, what do these ads that are being shown inside these  
15 mobile advertising libraries, what do they actually know  
16 about the user or what they can find out? In order to  
17 do this, we need to look kind of at them structurally,  
18 this whole ecosystem, and I promise I'll try to make it  
19 as painless as possible, although investigating it was  
20 fairly painful and involved a significant amount of  
21 reverse engineering, but it roughly looks something like  
22 this.

23 There are three kind of big parties in the  
24 picture, so there is that app, which is being shown on  
25 the phone. There is the advertising service, which is

263

1 supplying ads to the phone. And then there is the  
2 advertiser whose ads are being shown. And there has  
3 been a lot of work previously on trying to understand  
4 what information is available to the advertising  
5 service, but instead we are looking at what's actually  
6 available to the advertiser, and it's not the same  
7 question because there is a big difference between the  
8 advertising service and the advertising.

9 The advertising service is typically a  
10 reasonably respectable, reasonably reputable company  
11 that's maybe owned by, you know, Google or Twitter or  
12 some kind of recognizable entity. It is a large  
13 business. They have a reputation at stake. They make a  
14 lot of revenue.

15 Whereas advertisers are people who actually  
16 supply these ads that are being shown. Who knows who  
17 they are? I mean, this is dynamically determined. They  
18 are phished in real time, sold by auction, syndication,  
19 in all sorts of ways. These advertisers are not  
20 necessarily trusted. It's very hard to determine what  
21 information they're trying to extract.

22 And that's why mobile advertising libraries go  
23 to fairly significant lengths to protect users from  
24 malicious advertising and from snoop advertising -- from  
25 advertising that stealthily tries to extract information

264

1 about users. They use a variety of technical mechanisms  
2 to achieve this, and I'm not going to go into them. You  
3 can read our paper if you want to find out more about  
4 this.

5 The short summary is that what they try to do  
6 is they show every ad that they show to the user inside  
7 a little browser instance. So, there is a little web  
8 browser inside every advertising library, and they  
9 create a quote of this web browser every time they want  
10 to show an ad, and they show an ad inside of it.

11 And the good news about it is they, in effect  
12 -- they can effectively rely on security and privacy  
13 protections inside web browsers to protect phone users  
14 from malicious advertising. So, technically this is  
15 known as same origin policy, but you can think of it  
16 just as a way of sandboxing untrusted advertising to  
17 make sure it doesn't have any access with the underlying  
18 phone and cannot learn anything it's not supposed to  
19 learn from the phone.

20 And mostly it works, with one little  
21 exception. Mobile ads these days need access to what an  
22 Android phone is known as external storage, and the  
23 reason they need to do this is for rich media, because  
24 people who view advertising, especially people who  
25 supply this advertising, they want rich experiences,

265

1 they want video, they want images, and because of that,  
2 they need to cache a lot of information on the device,  
3 so they have access to external storage.

4 But to be safe, they allow ads to load files  
5 from external storage but not to read them. So, it  
6 cannot read it. It can just load it and show it to the  
7 user without being able to read it. So, that looks  
8 fairly harmless, except that Android external storage is  
9 kind of this weird thing. In Android external storage,  
10 there is really not a whole lot in the way of access  
11 control protections.

12 That is, if there are multiple apps running on  
13 the device and they store files in external storage,  
14 they can read each other's files. And that, you know,  
15 may not be ideal from the security perspective, but this  
16 should not really imply a whole lot about security and  
17 privacy of mobile ads, because as I told you, mobile ads  
18 cannot actually read other apps files from external  
19 storage. They can try to load them and try to show them  
20 to the user, but they cannot actually get access to them  
21 directly. They cannot look at their content.

22 So, so far so good. So, it seems like this  
23 whole way of protecting users from potentially malicious  
24 mobile ads is fairly carefully designed and carefully  
25 thought through, except that there is this one little --

266

1 I keep talking about this one little weird thing. They  
2 cannot read them, but they can try to load them. Why is  
3 this interesting?

4 It turns out that by trying to load a file  
5 that doesn't belong to them, mobile ads can learn a  
6 little bit. They can learn literally one bit of  
7 information. They learn if a particular file exists on  
8 the device or not. They cannot read it. They just  
9 learn if a file with a particular name exists. That  
10 seems like, okay, all right. That's fascinating. Why  
11 am I talking about this? Because that's really a very  
12 small amount of information.

13 So, now let's look at how this information  
14 might be used by a mobile ad. So, let's take an  
15 application which actually has nothing to do with mobile  
16 advertising, it's just a popular application in Google  
17 Play store that happens to be a drug shopping  
18 application. So, this allows people to go and look and  
19 reach pharmacists, drugs. You know, if somebody is  
20 taking a particular medication, they can find a pharmacy  
21 nearby where the price is lowest on it.

22 So, in this particular case, you can see there  
23 are some mitigations. There's particular things --  
24 actually, the fact that a person is taking one of these  
25 might be considered sensitive because these have to do

267

1 with anxiety and various psychological disorders.

2 So, what this app does, if a person is  
3 regularly shopping for a particular drug, they need it  
4 faster, it takes the picture of the pill, like the  
5 literal picture, like I'm showing here, and stores that  
6 picture in external storage on the device so that next  
7 time it's faster to show this picture.

8 Now imagine that there is an ad running in a  
9 different app on the same device, okay? It has the app  
10 that's showing the ad, but a totally random ad. It has  
11 nothing to do with that pharmacy shopping app that I  
12 showed you before; however, as I told you before, an ad  
13 being shown on it has the ability to ask a very simple  
14 question. Does a file with a particular name exist on  
15 the external storage? And in this case, it's asking for  
16 a file whose name corresponds to the image of one of the  
17 anxiety drugs.

18 So, what can a mobile app -- and this is a  
19 question to you guys -- what can a mobile app learn from  
20 the answer to this question? So, all it learns is one  
21 thing, if the file with a particular name exists on the  
22 device. What can the app learn by knowing the answer?

23 AUDIENCE MEMBER: That you order or you use or  
24 have some interest in this drug.

25 MR. SHMATIKOV: The only reason -- if the

268

1 answer to that question is yes, the only reason a file  
2 with this name would have existed on this device, if the  
3 user used that app and searched for that drug. There is  
4 no other reason. So, then if they see an -- if an ad  
5 sees that the file like this exists, it cannot read this  
6 file. All it needs to know that this file exists. It  
7 learns with hundred percent certainty, because this name  
8 is unique, that the person has been shopping for a  
9 particular drug.

10 And this turns out to be a pervasive problem,  
11 because -- and remember, this ad is being shown in a  
12 totally different app. It's not even being shown in the  
13 pharmacy shopping app. It's just being shown in some ad  
14 which is shown -- which is running on the device, maybe  
15 even later, not even at the same time as the pharmacy  
16 shopping app.

17 And this turns out to be a generic problem, is  
18 that if there is an app that need not even be  
19 advertising supporter, that puts files under external  
20 storage, like a lot of them do, in a way that depends on  
21 the user behavior, then an ad shown in any app on the  
22 same device can determine that this file exists, and  
23 from the fact that this file exists, it can infer what  
24 user behavior led to the presence of those files.

25 So, I have shown the example with drugs -- and

269

1 by the way, this violates nothing in the security  
 2 policy, because all the security policy says is that it  
 3 cannot read these files, and it cannot. It does not  
 4 read the file. It just learns that the file exists.  
 5 And this -- actually, it turns out that this  
 6 affects all kinds of mobile apps. Here is another app.  
 7 This happens to be a mobile web browser which caches  
 8 visited pages and files with predictable names.  
 9 Actually, the names of the files are derived from the  
 10 URL of the pages that the user visited, and it's  
 11 vulnerable to exactly the same attack.  
 12 A malicious ad running in another app can look  
 13 at the presence of certain files on the device, and it  
 14 can figure out which sites the user visited recently,  
 15 because the only reason a file with that name would  
 16 appear on the device is if it were cached by the user's  
 17 mobile browser as a result of a previous visit to a  
 18 particular website.  
 19 And in our paper, we have many more examples  
 20 about the inference that it could be done this way. We  
 21 actually did an analysis of several very popular  
 22 advertising libraries, including AdMob and MoPub which,  
 23 for instance, had a very significant fraction of Android  
 24 apps. They all, at least at the time of our study --  
 25 I'll tell you in a second what happened later -- have

270

1 this vulnerability, meaning that a mobile ad shown in  
 2 any of these libraries could infer information about the  
 3 user by presence of cached files raided by other apps.  
 4 We also looked in our study at other issues  
 5 like the leakage of location information. I'm not going  
 6 to go much into detail about this. I will just show you  
 7 this picture, and the only thing I want you to admire  
 8 about this picture is how complex it is, because it  
 9 shows, like, how in five stages, literally, in MoPub,  
 10 information about the user's location can be extracted  
 11 by an ad, but it works pretty reliably and doesn't  
 12 result in a mobile ad running in mobile, can create,  
 13 like, very nice trajectories of user movement like this,  
 14 which immediately reveals a ton of information about the  
 15 user, including actually the user's identity, if one of  
 16 these happens to be like a single-family residence where  
 17 the user lives. So, this is really fine-grain  
 18 information that can leak out through these  
 19 interactions.  
 20 Okay. So, what are the lessons of this study?  
 21 As far as I know, this is the first reasonably  
 22 comprehensive study of, first, how advertising libraries  
 23 on Android try to protect users from malicious mobile  
 24 ads and snooping mobile ads with intermediate success,  
 25 as you can see. It shows -- and this is a slightly more

271

1 technical result, but nevertheless important -- that  
 2 standard web isolation policies that are used in web  
 3 browsers, here are exactly the same things I used in the  
 4 mobile context, and they are no longer sufficient  
 5 because they no longer prevent leakage of sensitive  
 6 information. Something more subtle is needed here.  
 7 We actually, when we first did this study last  
 8 summer, we didn't make it public right away because we  
 9 actually wanted to work with developers of these  
 10 advertising libraries and companies that deploy them so  
 11 that they can fix at least the most severe  
 12 vulnerabilities that we identified, and, in fact, some  
 13 of them did, in particular AdMob, which is the biggest  
 14 Android advertising service -- actually, they're owned  
 15 by Google -- and they fixed that in the latest release  
 16 of their AdSDK.  
 17 Some library developers told us to go away and  
 18 not bother them anymore. I hope they won't do this  
 19 after this talk. And if you want more detail, we have  
 20 our paper online. It's written for a technical computer  
 21 science audience, but I hope at least the big themes  
 22 will come across from that.  
 23 Thanks.  
 24 (Applause.)  
 25 MR. ALVA: Next we will have Florian Schaub.

272

1 He is a post-doc fellow currently at Carnegie Mellon.  
 2 MR. SCHAUB: Hello, everyone.  
 3 I'm going to be talking about a project called  
 4 the Usable Privacy Policy Project, and this is a  
 5 large-scale project funded by the NSF under it's SaTC  
 6 program, and I'm a post-doc on this project. Norman is  
 7 actually the lead PI on this project, and it's a  
 8 collaboration with many people at CMU, Fordham  
 9 University, as well as the Center for Internet Society  
 10 at Stanford. And you can read more about the project at  
 11 our website, usableprivacy.org.  
 12 I'm going to give you a short evaluation and  
 13 then give you an overview of what we do in this project  
 14 in different parts. So, we look at privacy policies,  
 15 and privacy policies originally had this promise of  
 16 service providers would disclose the data practices so  
 17 users can then make informed choices about which service  
 18 providers or websites they trust with their data, but  
 19 the reality looks a little bit different, because  
 20 privacy policies play different roles for different  
 21 stakeholders.  
 22 So, for the service providers, it's not really  
 23 about informing the users. Most of them, when they  
 24 draft a privacy policy, the goal is to demonstrate legal  
 25 and regulatory compliance and in this way limit their

273

1 liability. And regulators are happy about this. They  
2 use these privacy policies to assess and enforce  
3 compliance.

4 So, there's actually a nice and strong  
5 interaction between those two players, but that means  
6 the user kind of gets left out. And as a result, these  
7 privacy policies are long, they're complex, they're  
8 difficult to understand, they're full of jargon, they  
9 don't really offer many choices to users, and I think we  
10 all know by now that users mainly ignore them.

11 This puts us in this really weird situation  
12 where these policies outline what companies do with our  
13 data and what we allow them to do with our data, but  
14 this information is not used by the users or made  
15 apparent to them.

16 And there has to be much work on overcoming  
17 the status quo here. Proposals like layered privacy  
18 policies, showing short summaries of policies, graphical  
19 approaches, as well as machine-readable privacy  
20 policies, but many of these approaches don't go anywhere  
21 really because they lack industry support and there are  
22 not sufficient adoption incentives for companies to  
23 actually implement those solutions that have been  
24 proposed.

25 This is where really our project comes in,

274

1 because we are looking at semi-automatically analyzing  
2 these natural language privacy policies that most  
3 websites, most mobile apps already have, and we analyzed  
4 them to then extract key data practices out of these  
5 policies, and we do this by combining crowdsourcing,  
6 machine learning, natural language processing, and this  
7 way enable large-scale analysis of privacy policies.

8 And at the same time, we look at modeling  
9 users' privacy preferences and concerns so that we can  
10 actually provide them more effective notices that focus  
11 on those information aspects and data practices users  
12 really care about and give them information that is  
13 actionable.

14 Our project has many tightly interconnected  
15 threads, and I'm not going to try to untangle this for  
16 you right now. Feel free to look at our report to get a  
17 deeper insight there. But basically we have two goals.  
18 One goal is we want to better inform users, we want to  
19 give them notices that actually inform them and provide  
20 them with choices, and we want to inform public policy  
21 by showing issues with privacy policies, as well as  
22 showing ways of remedying those issues and also  
23 providing -- hoping better notices could be provided.

24 And to identify data practices of interest, we  
25 approach it really from three different perspectives.

275

1 So, part of our research team looks at legal analysis.  
2 Joel Reidenberg and his team analyze privacy harms in  
3 litigation cases to see what issues come up the most. We  
4 conduct user studies where we determine what are privacy  
5 preferences, concerns and expectations of users. Ashwini  
6 this morning talked about some expectation work in that  
7 context.

8 And we also look at the policies themselves.  
9 So, how are they written? How are data practices  
10 actually expressed in those policies? We have some work  
11 going on right now that looks at quantifying the huge  
12 ambiguity and the vagueness of privacy policies.

13 To analyze these policies, we started by  
14 building an annotation tool that basically allows us to  
15 give policies to crowdworkers or other annotators, and  
16 this kind of tool shows them the policy on the left hand  
17 and then a question on the right, and we ask them to  
18 answer the question but also mark text that basically  
19 provides the evidence for their answer. And this is  
20 really important, because this text selection, in  
21 combination with the answer, then helps us build  
22 machine-learning models and frame machine-learning  
23 classifiers.

24 And by showing these questions or tasks,  
25 annotation tasks to multiple annotators, we can actually

276

1 get quite robust results; however, you know, just giving  
2 this to untrained crowdworkers and saying, oh, well, 10  
3 people say that's okay, is not really a good idea. So,  
4 we collected studies to compare the performance,  
5 annotation performance of experts who either write  
6 policies or have long experience in analyzing policies,  
7 graduate students in law and public policy and untrained  
8 crowdworkers recruited from Amazon Mechanical Turk, and  
9 we asked those people to annotate different privacy  
10 policies. The crowdworkers and skilled annotators and  
11 grad students annotated 26 policies, and then six of  
12 those policies were also annotated by experts.

13 I'm not going to go too much into the details  
14 for the sake of time, but one of the interesting results  
15 is that even the experts don't always agree on the  
16 interpretation of a privacy policy, and one reason for  
17 that is that the policies are vague but also that they  
18 are sometimes contradictory, and there are just too many  
19 different contexts handled in a single policy.

20 The good news is that for data collection  
21 practices, those are relatively easy to identify and to  
22 extract, they're usually in one part of the policy, but  
23 data-sharing practices are a bit more complicated. They  
24 are spread out throughout the policy. Sharing is  
25 mentioned in many different contexts and parts of the

277	<p>1 policies. So, it's kind of difficult to extract finer 2 nuances reliably.</p> <p>3 Now, when we compared the performance of the 4 crowdworkers to the skilled annotators, we actually find 5 quite encouraging results. So, when we hold the 6 crowdworkers to a certain quality standard, 80 percent 7 agreement, which means eight out of 10 crowdworkers need 8 to come up with the same interpretation, then we 9 actually find that in a large number of the cases, these 10 crowdworkers agree with the interpretation that our grad 11 students find as well. So, they come up with an 12 accurate interpretation.</p> <p>13 In almost all of the other cases, they don't 14 reach agreement, which means they don't give us wrong 15 answers. We have a very -- this dark bar shows us, it 16 is the percentage where they come to a different 17 conclusion than the skilled annotators. So, this is 18 great. So, either we get an answer from our 19 crowdworkers, and then with a highlighted group that's 20 actually correct, or we don't get an answer, and that 21 tells us that the policy might be too -- might be vague 22 on the particular issue we're trying to analyze.</p> <p>23 So, this shows that accurate crowdsourcing of 24 privacy policies is feasible, but privacy policies are 25 still long and complex. So, we look at leveraging</p>	279	<p>1 further split those tasks as well. So, rather than 2 asking them multiple questions at once, we first ask one 3 set of crowdworkers to kind of label in what category -- 4 what category of data practice is described. Is this a 5 sharing practice? Is this a collection practice? Is 6 this maybe about user access?</p> <p>7 And then in follow-up questions, we can ask 8 more details that is the particular aspects for that 9 kind of category. And that means that the task 10 interfaces we can show to crowdworkers are a lot more 11 compact and they can complete those tasks faster and 12 with lower errors.</p> <p>13 And based on that, we have developed an 14 annotation scheme that really makes use of this 15 approach. This is an interface not for crowdworkers. We 16 are using this with law students, but the next step is 17 to then break this up again with the product I just 18 outlined.</p> <p>19 But this is a very fine-grained annotation 20 approach, and we're currently collecting data from law 21 students. We already have over 100 policies annotated, 22 and this provides a really rich picture on how 23 information is represented, how data practices are 24 represented in the policies.</p> <p>25 We're going to release a data portal to allow</p>
278	<p>1 machine learning and natural language processing to 2 further enhance those extraction tasks and make it 3 easier for crowdworkers to complete these tasks faster 4 without loss of accuracy.</p> <p>5 And one approach we've tried to do or we've 6 been developing here is predicting and highlighting 7 relevant paragraphs. So, we take the answers we have 8 from our skilled annotators, and we use that to train 9 logistic regression-based relevance models for different 10 types of data practices we want to extract, and then we 11 highlight the top five, top 10 paragraphs that most 12 likely contain answers or information about the data 13 practices we want to extract. And what we find is that 14 that really helps the annotators to come to conclusions 15 faster without losing -- without affecting the accuracy.</p> <p>16 And we did additional experiments where our 17 analysis -- where we looked at do they actually just 18 focus on those five paragraphs or do they also read 19 other parts? And they do read other parts of the 20 policy, but it helps them to focus their search and find 21 parts in the policy again.</p> <p>22 Another thing we do is we split up this 23 relatively complex task of reading a privacy policy by 24 splitting the policy up in smaller paragraphs and then 25 giving a crowdworker only a single paragraph. We can</p>	280	<p>1 exploration of this data on Privacy Day this year, 2 January 28th. So, visit our website towards the end of 3 the month.</p> <p>4 And the nice thing about this data is it's 5 really helpful to train machine-learning and natural 6 language processing models and drive research in this 7 area.</p> <p>8 Ultimately, what we would be hoping for is 9 that we can actually automate the extraction, and one 10 approach we've been working on here is paragraph 11 sequence alignment. So, if I have a paragraph in one 12 policy, an Amazon policy, and this one is about 13 collection of contact information, and then if I compare 14 that one to a paragraph -- to other paragraphs in other 15 policies, there's a high likelihood that I can find 16 similar paragraphs that also describe the collection of 17 contact information, and this way we can basically 18 reduce which paragraphs we might not have to show to 19 crowdworkers and this way automate some of the 20 annotations and analysis.</p> <p>21 Now, once we have all this data, we want to 22 provide notice to users, and here we focus on making 23 sure the information we give users is actually relevant. 24 So, we highlight unexpected practices, practices users 25 care about, and information should be actionable. If</p>

<p style="text-align: right;">281</p> <p>1 users can't make a choice, then there's no point in 2 showing them information, because they're just going to 3 be helpless. We heard about this this morning, about 4 users becoming resigned because they can't make any 5 choices. 6 So, what we do is -- what we want to do is we 7 want to show them the choices that are made available in 8 the privacy policy -- there aren't that many -- but 9 because we can scale up this analysis to many websites, 10 we can also show more privacy friendly websites as 11 alternatives to users and in this way offer them choices 12 that go beyond the policy of what a single website might 13 offer. 14 And we're currently in the process of 15 developing a browser plug-in to basically make this 16 technology available to users, and the idea is that we 17 display a limited set of relevant practices, and we're 18 going through an iterative design process at the moment 19 with focus groups and online studies, but hope to be 20 able to release this plug-in to the public this summer. 21 So, in conclusion, what we do in this project 22 is we semi-automatically analyze privacy policies, and 23 we do this with crowdsourcing, with natural language 24 processing, and machine learning. And the goal of our 25 project is really to enable large-scale analysis of</p>	<p style="text-align: right;">283</p> <p>1 probably appreciate how much progress is actually being 2 made -- we have been able to make over the past few 3 years in both modeling and predicting people's privacy 4 practices, and so this talk is about sharing some of 5 these results with you and showing you also how this 6 effectively supports revision of developing personalized 7 privacy assistants; in particular, the success or at 8 least the early success we've had with mobile apps in 9 particular, and how this, we believe, can be extended to 10 IoT. 11 So, this is joint work with a large team that 12 will be acknowledged on the very last slide. I don't 13 think that I am going to have to work very hard to 14 convince this audience that people care about privacy, 15 and yet as we all know, also, people are often very 16 surprised when you tell them, for instance, what sorts 17 of apps they have downloaded on their mobile phones and 18 what information is being collected or shared by these 19 apps. 20 This is just an example of an early study we 21 conducted in this space. The biggest offender in that 22 case was an app that some of you at the FTC are quite 23 familiar called Brightest Flashlight, and 95 percent of 24 the people who had that app were extremely surprised and 25 very upset to find out what information that app was</p>
<p style="text-align: right;">282</p> <p>1 these privacy policies. 2 So, at the moment we are annotating 100 3 policies. In a year, we are hopefully annotating a 4 thousand policies and we are doing it at the same cost 5 or even cheaper. That's the idea. 6 And at the same time, we're really interested 7 in understanding what users care about so we can on the 8 one hand focus the analysis, but also help regulators 9 focus their activities potentially to look at those 10 issues users care about or are concerned with. 11 We want to show ways to effectively inform 12 users about the data practices that are currently lost 13 in those policies. No one is going to read the 14 policies. So, if you want to make those policies 15 usable, we need to extract the information that is 16 really relevant to users and show it to them in a format 17 that actually makes sense to them and actually allows 18 them to act on it. 19 Thank you. 20 (Applause.) 21 MR. ALVA: And our last presenter of the day 22 will be Norman Sadeh. Norman is a professor in the 23 School of Computer Science at Carnegie Mellon. 24 MR. SADEH: Well, good afternoon. 25 I think very few people in this audience</p>	<p style="text-align: right;">284</p> <p>1 actually collecting. 2 And, so, as we all know and as Florian just 3 emphasized again, very few people read privacy policies, 4 and that's sort of the reason why we have this level of 5 surprise. Also, as I think we are also realizing, many 6 of us have tons and tons of settings and just don't have 7 the time to configure all these settings. 8 For instance, if you are a smart phone user, 9 and as most smart phone users, you probably have 10 somewhere between 50 and 100 apps on your phone. These 11 apps typically will require between three and four 12 permissions. These are permissions to access some of 13 your more sensitive information. If you do the math 14 very quickly, you realize that this would require people 15 to configure somewhere around 150 different settings. 16 How many people are willing to configure 150 settings on 17 your cell phone? Not that many. 18 And, so, with this in mind, and obviously with 19 a recognition of these challenges both already on the 20 fixed Internet and in the mobile space, the natural 21 question is, well, if this already doesn't work on the 22 fixed web, if this already doesn't work on the mobile 23 web, what are the chances that it's going to work in 24 IoT, with the Internet of Things? 25 And, so, our vision in this space, as I said,</p>

285

1 is this idea that perhaps personalized privacy  
2 assistants could be developed that will actually reduce  
3 the burden and allow you to manage your privacy better  
4 across these different environments.

5 And, so, the idea is that this personalized  
6 privacy assistants in particular will learn over time  
7 your privacy preferences and will be able to  
8 automatically configure many of those settings based on  
9 various correlations between how you feel about sharing  
10 your information with one app versus another app; based  
11 on also understanding what your expectations are, going  
12 back to the presentation that was given this morning by  
13 Ashwini Rao, who has been looking at these issues.

14 In particular, for instance, if you think, as  
15 Florian also mentioned about privacy policies, when you  
16 read these privacy policies, they tend to be very long,  
17 very verbose, but very often at the end of the day  
18 there's only a very tiny fraction of that text of that  
19 policy that matters to you, and perhaps even a tinier  
20 fraction of the text that pertains to things that you  
21 didn't already expect.

22 And so perhaps these personalized privacy  
23 assistants could help us actually highlight -- could  
24 help us by highlighting those elements of policies that  
25 really would be a surprise to us, that perhaps would

286

1 lead us to modify our behavior as we enter a smart room,  
2 for instance, in an IoT context.

3 Perhaps these personalized privacy assistants  
4 could also help motivate users to revisit some of their  
5 settings to verify that they still feel the same way.  
6 Privacy preferences are not fixed. They might change  
7 over time based on your experience, based on what you  
8 learn.

9 And, so, again, what I would like to do is I  
10 would like to share with you some of our success that is  
11 actually supporting some of the early elements of this  
12 functionality. What you are seeing here is effectively  
13 an early model that we built about how people felt  
14 sharing their information with various mobile apps for  
15 various types of purposes, whether the app requires this  
16 information for internal purposes, for sharing with  
17 advertising networks, for profiling purposes, or for  
18 sharing with social networks.

19 I'm not going to describe this chart in great  
20 detail, because time is limited, but effectively what we  
21 are supposed to see here is that people don't always  
22 feel the same way on average when it comes to sharing  
23 their information. There are clearly differences  
24 between sharing location information at a fine level  
25 versus sharing it at a coarse level. There are

287

1 differences when it comes to sharing, for instance,  
2 access to an SMS functionality and certainly depending  
3 on whether you are going to be doing that for  
4 advertising purposes versus using it purely for the  
5 purpose of the app that you are trying to download.  
6 People are going to feel very differently.

7 What this figure, however, doesn't show is how  
8 difficult it is to actually configure settings, and the  
9 reason why it's difficult to configure settings is that  
10 this chart here, as you see it, is not the whole story.  
11 The whole story actually comes out when you start  
12 looking at this other chart, which shows you the  
13 standard deviation when it comes to these preferences.

14 And, so, the story here and the reason why  
15 privacy is so complex is that we don't all feel the same  
16 way about these issues. If we did, it would be simple  
17 to come up with defaults and use these defaults for the  
18 entire population, and then we would be done, and  
19 perhaps even the FTC could jump in and say, well, nobody  
20 feels comfortable about this; therefore, we are going to  
21 outlaw it. Clearly that is not the way we operate.

22 And, so, the reason why this is complex is  
23 because we have this diversity in preferences. Some  
24 people are quite fine with their fine location being  
25 shared with advertisers and others object. The good

288

1 news, however -- and this is a result that has come out  
2 from research over the past years -- is that very often  
3 it is possible to organize the population and their  
4 preferences into a fairly small group of people, fairly  
5 small groups of people that feel very much the same way  
6 about these issues.

7 And, so, what I want to share with you here  
8 is, again, an early example of our work in this area,  
9 where, again, looking at these mobile app permission  
10 preferences, we're able to organize a population of  
11 users in just four groups, and just based on these four  
12 groups and what we're able to predict based on the  
13 preferences within each of these four groups, we're able  
14 to show that it might be possible to predict somewhere  
15 between 75 and 85 percent of their pricing preferences  
16 when it came to configuring their permission settings.

17 And, so, this is very, very simple technology.  
18 I'm going to show you that we've been able to go much  
19 farther than that. But that gives you a sense already  
20 for how easy it is actually to predict many different  
21 settings that perhaps people would want to have.

22 So, this next chart here shows you the next  
23 step in our research in this area, where we looked at  
24 actually a population of 240,000 users. I should  
25 actually say a population of 3 million users, but we had

72 (Pages 285 to 288)

289

1 to clean up the data quite a bit, and we eventually  
 2 zoomed in on the fraction of the population that was  
 3 most engaged with their permission settings.  
 4 So, these were users who were using a  
 5 variation of the Android operating system. It was a  
 6 nerdy version of Android where users could actually  
 7 configure many different settings. And we were able to  
 8 show that through profile levels or through personalized  
 9 learning, we could just, by asking people a very small  
 10 number of questions, effectively predict most of the  
 11 settings that they would need to configure on their  
 12 smart phones for the apps that they were going to  
 13 download.  
 14 So, for instance, if you were to ask them just  
 15 six questions, you could effectively reach a level of  
 16 accuracy of about 92 percent. If you're willing to  
 17 double the number of questions you are asking, you're  
 18 getting close to 95 percent.  
 19 Now, we are not suggesting in any way that you  
 20 should fully automate the setting of privacy  
 21 permissions. We strongly believe in dialogues with  
 22 users, but there are situations where it's extremely  
 23 clear of how the users feel about some settings, and  
 24 there are situations where you can determine that  
 25 actually your model is not good enough to predict what

290

1 those settings should be, and that's where you should  
 2 ask the user, right? And that's effectively what we are  
 3 advocating.  
 4 And, so, we have gone one step further this  
 5 past summer, and we actually piloted this technology  
 6 with real users on their actual cell phones. So, we  
 7 developed profiles. In this case, we came up with  
 8 several different profiles and asked people to download  
 9 this very early version of a personalized privacy  
 10 assistant.  
 11 This assistant would ask them between three  
 12 and five questions based on the actual apps they had on  
 13 their cell phones, and based on their answers, it would  
 14 recommend a number of different settings, as you can  
 15 potentially see on the right-hand side of the slide in  
 16 front of you.  
 17 And, so, we ran this, and to make a long story  
 18 short, we ran this for effectively a period of 10 days.  
 19 The last six days of the study, we actually tried and  
 20 see if we could nudge users to modify the settings that  
 21 they had adopted based on recommendations made by these  
 22 assistants. We tried very hard with nudges like the one  
 23 you see here. These nudges are very effective, by the  
 24 way.  
 25 So, when it comes to getting people to rethink

291

1 their privacy preferences, when it comes to motivating  
 2 them, we've actually got an entire study that shows that  
 3 those types of nudges work very well.  
 4 And, so, here's what we found. We found that  
 5 among the recommendations made by the personalized  
 6 privacy assistants for the mobile apps, about  
 7 three-quarters of motivations were adopted by users, and  
 8 we also found that even after they adopted these  
 9 recommendations and modified their settings based on a  
 10 recommendation, even though we were trying very hard to  
 11 get them to revisit these settings, they would not  
 12 change them. That means that in this case, about 5.6  
 13 percent of those recommendations were later modified,  
 14 despite nudges that we're sending them to revisit and  
 15 rethink their settings.  
 16 Now, how do we know -- you might say perhaps  
 17 they were just lazy, perhaps they ignored your nudges.  
 18 Well, we had intentionally come up with recommendations  
 19 that were ignoring a number of other settings. And, so,  
 20 the nudges also covered settings that we had not covered  
 21 in the recommendations. And those settings, users were  
 22 actually modifying. So, we know that they were actually  
 23 truly engaged. And, so, this suggests to us that these  
 24 recommendations are actually pretty close to how people  
 25 feel about these issues.

292

1 And, so, we strongly believe that this is the  
 2 way to go for mobile apps. The question is, could we go  
 3 one step further and could we generalize this to IoT?  
 4 And, so, we have started to work in this area. The  
 5 vision here is that you would extend this to deal with  
 6 smart spaces.  
 7 And, so, what we are doing right now is we are  
 8 building an infrastructure where owners of different  
 9 resources, resources that are going to be sensing  
 10 different aspects of your behavior -- cameras, location,  
 11 present sensors and the like -- those resources have to  
 12 be defined in the register by the owners, the people who  
 13 own these various resources.  
 14 You know, if you enter a room like this, there  
 15 are actually a number of different people who might  
 16 potentially have deployed different resources already  
 17 today that collect some of your information. For  
 18 instance, it could be the case -- I hope it's not the  
 19 case -- but it could be the case that the WiFi routers  
 20 in this room perhaps collect your information.  
 21 These WiFi routers are not necessarily owned  
 22 by the people who operate the building. Perhaps they  
 23 are owned by the FTC, perhaps they are owned by a third  
 24 party, I don't know, and perhaps it's better not to ask.  
 25 But on the other hand, the HVAC system in this building

73 (Pages 289 to 292)

293

1 might be owned by an entirely different entity, and that  
2 HVAC might be collecting information, too.

3 So, I think that the owners of these resources  
4 should be able to very simply declare where these  
5 resources are deployed and what information these  
6 resources collect and all the other sorts of attributes  
7 that you would ideally want to see in a privacy policy.

8 So, we're developing an infrastructure where  
9 through a series of dropdown menus, people can specify  
10 different elements of their resources without requiring  
11 them to do any programming and look at what it takes to  
12 turn these -- this information into machine-readable  
13 privacy policies.

14 The idea is that users then, with their  
15 personalized privacy assistants, would be able to enter  
16 the space, discover relevant resources. Their  
17 assistants would determine, based on their expectations  
18 and their preferences, what, if anything, they need to  
19 be warned about or informed about. And if there happens  
20 to be settings in the ideal world, we would like these  
21 personalized privacy assistants one day to also  
22 configure these settings. We're not there yet, but  
23 that's effectively what we're aiming for. So, this is  
24 roughly how this is hopefully going to work one day.

25 So, let my try to quickly recap and also make

294

1 some connections with public policy in this space. So,  
2 we truly believe that this approach to effectively  
3 leveraging machine learning, in particular, building  
4 personalized models of people's privacy preferences and  
5 expectations, is one way of making notice and choice  
6 practical, right?

7 Today, the number of systems that you are  
8 encountering, especially in the IoT context, is just way  
9 too great for anyone to imagine that users are going to  
10 be able to read policies or configure settings. There  
11 is really a need to help users and to really do so by,  
12 number one, building models of what they care about; how  
13 they feel about different sets of issues; try to  
14 effectively alleviate burden in that context; and also  
15 make it much easier for the various owners of different  
16 elements of the infrastructure in the IoT context to  
17 participate within this infrastructure.

18 So, as was pointed out by Sarthak, I think, in  
19 the first presentation on this panel, one of the  
20 challenges of IoT is a diversity of players. If you  
21 think about the way you interface with a fixed Internet,  
22 most of your interactions are mediated by the browser,  
23 and so it's efficient in principle to just configure  
24 settings in your browser. On the mobile web, by and  
25 large, the cell phone mediates your interaction,

295

1 Android, and so it's sufficient to configure a number of  
2 settings at that level.

3 In IoT, it's a very different story, right,  
4 where you have a number of different players that might  
5 contribute different elements of the infrastructure.  
6 Many of these players might also be smaller entities  
7 don't have the sophistication that Google or Microsoft  
8 or Facebook might have. And so we really need to move  
9 towards an open environment, with open APIs, where  
10 effectively people will expose settings that will enable  
11 one, through personalized privacy assistants or  
12 equivalent technology, to effectively configure many  
13 settings on behalf of the user. And so that's really  
14 our vision in this space.

15 You can think of two different ways of  
16 deploying this personalized privacy assistant  
17 technology. One is to effectively rely on companies  
18 like Google or Facebook, each one of them potentially  
19 developing its own personalized privacy assistant,  
20 building models of the users. You can imagine also some  
21 potential tensions or potential conflicts of interest  
22 when it comes to theories that we have to come up with  
23 based on various guarantees.

24 Or, you could imagine a more ambitious effort  
25 where you might say, well, after all, there are some

296

1 interesting correlations between the way you feel about  
2 your settings on mobile apps, when it comes to sharing  
3 information with mobile apps, and perhaps your settings  
4 on Facebook and perhaps your settings in your browser.

5 And, so, rather than asking you these five or  
6 ten questions in each one of these environments in order  
7 to determine what your privacy preferences are, how  
8 about just asking you these questions perhaps just once  
9 and using your personalized privacy assistant, that cuts  
10 across all these different environments, interact with  
11 these open APIs to effectively configure many of these  
12 things on your behalf.

13 So, that's our vision in this space. It's not  
14 guaranteed that these APIs will be made open. In fact,  
15 today, they are not. They are very much part of the  
16 strategy that some of these larger entities have when it  
17 comes to building their own systems, but we would like  
18 to effectively build an effort towards perhaps  
19 convincing these larger players that they would all  
20 benefit from opening up these APIs, and perhaps people  
21 will ask me questions later on so I get to say more  
22 about this, but I think I have run out of time.

23 So, thank you very much.

24 (Applause.)

25 MR. ALVA: We'll conclude today with our final

297

1 discussion of the day. Unlike previous sessions that  
2 have focused mostly on privacy, this session has focused  
3 on security and usability, research as it relates to  
4 privacy.

5 Sarthak discussed security issues related to  
6 IoT devices, and how they may affect privacy in the  
7 home. Vitaly presented on ad libraries and how the lack  
8 of tailored security controls in some contexts could  
9 result in disclosure of users' information through  
10 shared external storage.

11 For usability, Florian shared about an entire  
12 line of research going on around using machine learning,  
13 crowdsourcing, and other methods to make privacy  
14 policies more usable and for consumers, for businesses,  
15 as well as maybe for regulators. Finally, Norman  
16 presented new ways to understand and manage users'  
17 privacy expectations through personal privacy  
18 assistants.

19 Overall, this session has provided some new  
20 views into different strands of privacy research to  
21 consider. Now we will add to the policy conversation  
22 through our conversation here.

23 I want to welcome Geoffrey Manne, the  
24 Executive Director of the International Center for Law  
25 and Economics, as well as its founder, and Davi

298

1 Ottenheimer, who holds many hats in the security  
2 community, including authoring a book on big data  
3 security.

4 Geoffrey and Davi will provide some thoughts  
5 on this session as it relates to privacy for a few  
6 minutes each, and we will start there.

7 Geoff?

8 MR. MANNE: Thanks, Aaron. So, I thought the  
9 papers presented some really interesting things, and as  
10 did the papers throughout the day, and since this is the  
11 last session and I have you here, I am going to talk a  
12 little bit more broadly at first, anyway, than just  
13 about the papers today, but in a way that's consistent  
14 with what Aaron was saying, which is to say that the  
15 papers are interesting, there's some really important  
16 stuff here, but as is so often the case, the problem is  
17 deriving the appropriate policy implications from it.

18 One of the things I would say is that it's a  
19 little bit unfortunate, we don't have more economists  
20 and engineers talking to each other. As you might have  
21 gathered from the last panel, an economist will tell you  
22 that merely identifying a problem isn't a sufficient  
23 basis for regulating to solve it, nor does the existence  
24 of a possible solution mean that that solution should be  
25 mandated.

299

1 We really need to identify real harms, rather  
2 than just inferring them, as James Cooper pointed out  
3 earlier, and we need to give some thought to self-help  
4 and reputation and competition as solutions before we  
5 start to intervene.

6 Now, it is certainly something in the nature  
7 of a conference like this, and for that matter, the  
8 kinds of papers that people are writing, because  
9 journals don't publish papers saying there's nothing  
10 wrong. They publish papers saying, you know, there's a  
11 problem, and perhaps suggesting solutions to them.

12 So, we've talked all day about privacy risks,  
13 biases in data, bad outcomes, problems, but we haven't  
14 talked enough about beneficial uses that these things  
15 may enable. So, deriving policy prescriptions from  
16 these sort of lopsided discussions is really perilous.

17 Now, there is an additional problem that we  
18 have in this forum as well, which is that the FTC has a  
19 tendency to find the justification for enforcement  
20 decisions in the things that are mentioned at workshops  
21 just like these. So, that makes it doubly risky to be  
22 talking even about these things without pointing out  
23 that there are important benefits here and that the  
24 costs may not be as dramatic as it seems because we're  
25 presenting these papers describing them.

300

1 So, to think about the potential  
2 vulnerabilities that we talked about on this panel, the  
3 question to me becomes should they lead the FTC to any  
4 kind of enforcement if companies don't engage in the  
5 type of security that was recommended in some places or  
6 even any security at all?

7 And, again, this is an FTC workshop, so  
8 counselors out there are actually going to have to  
9 wonder if their companies are now on notice and if the  
10 very selection of papers for presentation here perhaps  
11 indicates anything about the FTC's enforcement agenda.

12 But here's the thing, having a possible  
13 vulnerability and acting unfairly under Section 5 are  
14 not the same thing. And, by the way, that's  
15 essentially, I think, the holding in the ALJ's decision  
16 against the FTC in the LabMD case.

17 Also, in terms of the desirability of  
18 enforcement, I think it's important to note that a  
19 couple of papers in this session and elsewhere  
20 throughout the day have suggested either that self-help  
21 is or can be working -- Norman's paper most obviously  
22 and immediately suggested a version of that -- or that  
23 despite the potentiality of all of these problems,  
24 something is actually preventing these vulnerabilities  
25 from being dramatically exploited.

301	<p>1 Self-help has direct legal implications, say, 2 for a deception claim, where it matters if it's 3 available, but both self-help and the limited 4 exploitation of risks are important in the economic 5 calculus of the desirability of enforcement. 6 So, I want to end really quickly by saying I 7 have more specific questions and comments about the 8 papers when we discuss, but overall, I would just like 9 to say that I think that last point is an area in which 10 we're lacking in research, and I would like to see 11 significantly more research on the implications of the 12 availability of self-help, and what are the incentives 13 for consumers themselves? 14 We've spent all of our time talking about the 15 incentives of firms and the implications of legal 16 liability on firms, but what about the consumers 17 themselves? What about self-help? And how does and 18 should the FTC take account of those? 19 MR. ALVA: Thanks. 20 Davi? 21 MR. OTTENHEIMER: All right. Well, I feel 22 like somebody has given me a big basket of balls to 23 juggle here at the end of the day. I will try to make 24 sense of it all, a little bit of a show. 25 Teeing off on what Geoff just said, the idea</p>	303	<p>1 people to make big analytic analysis; it's really small. 2 And that's kind of the two ends that I see. 3 And then the fourth speaker, even more 4 interestingly, has a shared model, where not only are 5 you making things easier to decide, accuracy and choice, 6 but you're encouraging, nudging people. So, you're 7 bringing an economic model towards the middle, towards 8 simpler decisions with nudges. So, that's kind of how I 9 see the four put together. 10 And I guess I have a ton of questions for all 11 the speakers, but we don't have that much time, so I'll 12 give it back. 13 MR. ALVA: Thanks. 14 So, I wanted to ask -- since we're running out 15 of time, I wanted to ask a general question across all 16 of the presenters. If there is one policy message that 17 you think currently your research is engaging in, as you 18 discussed in your presentations, but is lacking in 19 technical measures that would actually help you 20 implement the policy goal you would like to see, what 21 are those shortcomings and how are you or would you like 22 those shortcomings addressed? 23 And this question is open to any of the 24 presenters. 25 MR. SADEH: Okay, it's a tough one. Clearly,</p>
302	<p>1 that there are these experiences we can have and we can 2 learn from and there are these things we can discover 3 through hard science is a fair split, and I will apply 4 it now to the talks we heard today, the four talks. 5 I think that goes back to the question, should 6 you study computer science or should you study social 7 science? Should you have an applied approach to risk or 8 should you have an academic approach? And a lot of 9 times people forget that there's something in the 10 middle. There is a fair balance between the two. 11 So, it was interesting to me to hear the first 12 speaker talk about one end of the spectrum, which is 13 essentially unit tests of these devices, these IoT 14 devices; and then the second speaker took us through an 15 integration test, a scenario asking what are these 16 devices like in the wild? Let's look at how they're 17 used by people, the economics, essentially the social 18 science of how they're used. So, those are two ends of 19 the spectrum, essentially. 20 And so then the third and fourth speakers 21 brought in the middle ground, where you have somebody 22 saying, well, maybe we can use this analytic exercise to 23 help people make small rational decisions, right? So, 24 you reduce the decision set criteria so people can 25 choose from something realistic. So, you're not forcing</p>	304	<p>1 one has to be realistic about what can be done and how 2 much room for maneuver I guess the FTC has in this 3 space, but I suspect that the FTC can play a role in 4 bringing together key stakeholders and encouraging 5 dialogues. 6 And so, for instance, the issue that I was 7 alluding to at the end of my talk, for instance, in 8 terms of opening APIs, clearly this will never be 9 something that, you know, one would ever be able to 10 mandate, but perhaps efforts can be encouraged by 11 bringing together key stakeholders. 12 At the end of the day, when privacy is 13 prevented the right way and when people are looking at 14 this rationally, everyone can benefit from better 15 privacy, including vendors that, you know, are sometimes 16 presented as if they didn't care about privacy. If you 17 look, for instance, at what is happening today in the 18 mobile space, it's very clear that everyone has come to 19 realize that they don't want to be seen as the people 20 who don't care about privacy, and that creates strong 21 incentives for them to rethink the way in which they've 22 been approaching some decisions in that space. 23 So, I think that perhaps the FTC can, on the 24 one hand, continue to do what it's been doing very well, 25 I believe, which is to encourage best practices, that it</p>

305

1 has done, for instance, for mobile apps, as it has done  
2 more recently when it comes to IoT security, and perhaps  
3 also convening meetings and encouraging efforts where  
4 people look at opportunities for perhaps developing  
5 common standards, not trying to impose any standards,  
6 and, you know, standards are very challenging and very  
7 tricky efforts, but at least trying to bring together  
8 key stakeholders and trying to get them to think about  
9 where they've got effectively common interests and where  
10 they might benefit from perhaps developing some open  
11 APIs.

12 MR. SHMATIKOV: I think transparency is very  
13 important. Better understanding and better disclosure  
14 of how information is collected and shared between  
15 various players in the picture is crucially important,  
16 because what we have in mobile space today is these old  
17 permission models. They capture something about  
18 security of these devices. They capture virtually  
19 nothing about privacy.

20 There is a lot of information collection and  
21 sharing and information used between all kinds of  
22 artists -- platform operators, ad libraries, ad  
23 builders, advertisers -- that simply exists outside the  
24 existing permission models that a lot of privacy work  
25 focuses on. So, to the extent FTC can help shed light

306

1 on this and ask for more disclosure of information  
2 collection practices and information flows in this  
3 massive mobile ecosystem, that would be an extremely  
4 useful service, because that is not happening today.

5 MR. GROVER: So, I would totally agree with  
6 that. Transparency is the big issue, and maybe, like,  
7 the FTC can, in terms of IoT devices or mobile apps, say  
8 unless you follow a certain set of policies, we won't  
9 allow you to sell these devices to others.

10 But the problem comes back to a point Norman  
11 mentioned, that in terms of IoT devices, there are not  
12 really open APIs, and, I mean, who basically sits there  
13 and looks at all of this? Who does the analysis when  
14 you don't really have access to the code? And when the  
15 software and the hardware are basically integrated, you  
16 don't have choices in case you feel like something is  
17 wrong in the software. You aren't really able to  
18 replace it with something else.

19 So, transparency is the main issue, and it  
20 should be encouraged, but, quite frankly speaking, I  
21 don't know how to go about it. That's the problem.

22 MR. MANNE: So, but, you know, one of the  
23 things -- I mean, there's always tradeoffs. It may not  
24 surprise you all that Leonard and I wrote a paper called  
25 "The Cost of Disclosure," so I agree transparency tends

307

1 to be a good way of achieving these things, but it's not  
2 costless. As Norman had on his last slide, he pointed  
3 out that if we have open APIs, we're going to be  
4 empowering the groups that are collecting these massive  
5 amount of information through open APIs with an enormous  
6 amount of information that creates perhaps even greater  
7 vulnerabilities than the ones we're protecting. So --  
8 and there may be other examples like that, too.

9 So, my question really is, before we settle on  
10 transparency, even, as the right sort of, you know,  
11 optimal kind of solution here, we should be aware that  
12 there are costs to that as well, and, again, potentially  
13 we're creating more risks than we're solving.

14 MR. OTTENHEIMER: That's right. I put it as,  
15 transparency to whom? So, transparency -- you know,  
16 you're building trust relationships, so it's  
17 transparency to somebody that you essentially trust to  
18 give you the right answer, and given that they have the  
19 information. So, I've done audits over 20 years, and I  
20 can tell you, just being able to see into something  
21 doesn't mean you're in the position to make the decision  
22 on it, which is sort of what the presentations were  
23 about to some degree.

24 We give the people the information. The  
25 people are positioned in a way that they can't digest it

308

1 because they don't have the analytic capability at the  
2 time they're given the information. That's why I'm  
3 saying balance. If you take the sort of unit tests, you  
4 can say that's inadequate because you have a compliance  
5 checklist. If you take the environmental or the  
6 integration test, you can say, well, that's not fair  
7 because that's not a typical use case.

8 So, somewhere in the middle is proper use of  
9 the device prepared for a use case, and that's I think a  
10 good fit.

11 MR. SCHAUB: So, I think concerning  
12 transparency, an interesting point to think about is  
13 essentially the privacy policies we have right now,  
14 they're not written for users, and they're not meant to  
15 provide transparency for users, and we need to realize  
16 this and I think this needs to be more clearer in  
17 regulation as well, that if we want to inform users and  
18 achieve transparency for users, then we need to come up  
19 with user-facing notices that are actually made for  
20 users.

21 That could include requiring user evaluation  
22 of those notices. Are they actually effective at  
23 communicating what they are supposed to communicate? And  
24 we've been doing a lot of those studies at CMU, and we  
25 find most notices are not effective, and it's really

309

1 hard to design an effective notice.  
 2 MR. OTTENHEIMER: Here's the interesting  
 3 counterpoint. The more information that becomes  
 4 available, the more behavior changes. So, if you  
 5 actually -- I could show you exploits, for example, to  
 6 your model that show as you get this in position where  
 7 your machine-learning algorithms are working and you're  
 8 actually getting the answers you want, the people  
 9 writing the policies will change them just so you can't  
 10 see them anymore.

11 So, the transparency has been to be in concert  
 12 with the right trust model where people want it to be  
 13 shown in the way that it's comfortable for them;  
 14 otherwise, they adapt and your transparency backfires.

15 MR. ALVA: Norman, did you want to address the  
 16 transparency --

17 MR. SADEH: Well, I would like to respond to  
 18 the last comment. So, I think it's clear that privacy  
 19 is an arms race, right? So, I think that Davi and I  
 20 worked with Florian on the project that he described,  
 21 but the day that site operators, for instance, start  
 22 modifying their policy based on our technology, because  
 23 of the success of our technology, will be a very good  
 24 day. We're not quite there yet.

25 If that day happens, we will actually have the

310

1 ability to probably identify that, and that might  
 2 potentially be something that the FTC would be  
 3 interested in. Whether the FTC would actually be able  
 4 to do very much about it or not, I'm not sufficiently  
 5 versed into the legal ramifications of that, but I  
 6 suspect that it would have something to say if you can  
 7 establish effectively a pattern where, once you  
 8 effectively are able to capture some practices that are  
 9 not necessarily putting these companies in good light,  
 10 they start modifying the way in which they're presenting  
 11 the text, I suspect that's something -- you know,  
 12 something that could potentially be done.

13 MR. SCHAUB: And it's also quite imaginable  
 14 that it could go the other way, so that companies  
 15 actually improve their language to be better presented  
 16 by these independent mechanisms, and we have  
 17 conversations with many different companies that say  
 18 they would actually welcome having such kind of  
 19 technology out there, because they do invest a lot of  
 20 money and time in having privacy policies that are  
 21 descriptive.

22 But it's basically in vain at the moment  
 23 because this information is not used, and it's not clear  
 24 to users that this is the case. So, I think this could  
 25 go both ways, but it's going to be interesting to see

311

1 how it plays out.

2 MR. MANNE: I mean, my sense would be that the  
 3 primary reason for the unintelligibility of existing  
 4 disclosures of privacy policies is the legal risk and  
 5 for that matter even regulatory enforcement. So,  
 6 there's -- you know, if we're going to identify -- if  
 7 the problem is we don't have disclosures that actually  
 8 inform the users, then we haven't really -- to me, we've  
 9 largely identified a really important disconnect between  
 10 how we're regulating and, you know, the power of users,  
 11 which goes to the point I was making before, which is I  
 12 really liked what you were describing.

13 The sort of app that you guys created seems to  
 14 me like it has, you know, amazing potential, but once we  
 15 have something like that, think of what that does to the  
 16 need for additional forms of regulation. I mean, you  
 17 might still need some deception regulation, but you've  
 18 done a really good job now of actually giving users what  
 19 they want, and because users are so heterogeneous,  
 20 because types of data are so heterogeneous -- I think,  
 21 by the way, on your paper, there's a big difference  
 22 between an email address being accessible and the  
 23 content of a communication even with a computer device.

24 A real problem with overgeneralization -- and  
 25 this may be actually partly reflected in the bad privacy

312

1 policies -- a problem with sort of an overgeneral  
 2 response, like a network-level response to the problem  
 3 you were identifying, is that -- well, I don't know  
 4 enough about the engineering, but at first cut I would  
 5 say it doesn't differentiate; it just imposes a single  
 6 policy on everyone, regardless. That's really unlikely  
 7 to be the right outcome, but that is a problem with, you  
 8 know, sort of the more -- the blunt -- relatively blunt  
 9 policy tools that we have.

10 So, you know, again, I think there's real  
 11 value in empowering users as long as that leads to a  
 12 reduction in the incentive of these more blunt tools to  
 13 come in.

14 MR. ALVA: So, we have about 45 seconds left.  
 15 I wanted to ask the presenters, if you had the ideal  
 16 privacy agenda in your research, what would it be -- in  
 17 one or two sentences -- going forward?

18 MR. SADEH: I think I have outlined our agenda  
 19 and there were three presentations today, so I strongly  
 20 believe in this vision of personalized privacy  
 21 assistants. It's clearly not something where we are  
 22 entirely there yet, but we have some very promising  
 23 results.

24 If I can take another 30 seconds --

25 MR. ALVA: No, sorry. But thank you, though.

313

1 MR. SCHAUB: So, I think what's also  
2 important, when we are starting to look at this,  
3 providing information and integrating these dialogues  
4 into the users, into action flow. So, rather than  
5 having a privacy notice or privacy policy somewhere  
6 else, when the user interacts with it, make it part of  
7 the interaction.

8 The mobile platform developers are doing a  
9 good job doing this already or starting to do this  
10 already. You have those just-in-time dialogues that pop  
11 up, and they don't disrupt the interaction. They  
12 actually help it, and they actually encourage the app  
13 developers to build dialogues around it that tell you  
14 why this notification is going to pop up and why they  
15 want your location. So, that's great. I think that's a  
16 good direction to go in, to think -- we're doing quite  
17 interesting research on these things.

18 MR. SADEH: And we're not biased.

19 MR. ALVA: I'll stop you there. I encourage  
20 the audience to ask Vitaly and Sarthak after this, but I  
21 wanted to conclude.

22 So, the FTC's new chief technologist started  
23 on Monday, and so I wanted to welcome Lorrie Faith  
24 Cranor from the FTC, and we also thank Carnegie Mellon  
25 for allowing her time on leave for her to be here with

314

1 us.

2 MS. CRANOR: Thank you. I will keep my  
3 remarks brief, since we are over time.

4 First of all, I wanted to thank all of the FTC  
5 staff who did such a wonderful job organizing this  
6 event. Can we give them a big round of applause?  
7 (Applause.)

8 MS. CRANOR: So, this is my fourth day, so I  
9 had nothing to do with it, but these guys did a really  
10 great job. I also want to thank all of you for coming  
11 and for participating.

12 A few notes on some things that I heard  
13 throughout the day. It was a lot to absorb, and I was  
14 busy scrolling notes and trying to synthesize what I  
15 heard.

16 So, I think some of the key areas that I  
17 heard, there's a lot of really interesting empirical  
18 research that is being done and some of the areas that  
19 it's being done in that we heard about. We heard about  
20 survey and interview research about what consumers  
21 understand and especially what they expect and what they  
22 desire.

23 We also saw that some of this research is then  
24 being used to find ways to actually assist consumers,  
25 figuring out ways to reduce the number of notices that

315

1 they need to see, and configure their settings  
2 automatically.

3 A question that came up in almost every panel,  
4 I think, was a question about how we can make  
5 transparency and notice and choice more effective. We  
6 heard over and over again how ineffective it seemed to  
7 be, and we heard some ways forward, some paths to maybe  
8 making it more effective.

9 We also heard about measurement research that  
10 looked at a variety of things. We heard about  
11 measurements on the extent that people are being tracked  
12 and what technologies are tracking them. We also heard  
13 about statistical and machine-learning research to  
14 understand how algorithms impact users.

15 And our speakers observed that in order to  
16 have algorithmic transparency, it's not enough to just  
17 know what the algorithms are, because that doesn't  
18 really tell us very much. What we need is systems that  
19 help interpret the results of the algorithms and show us  
20 the impact of those algorithms.

21 We saw some research that the models have  
22 investigated the impacts of different approaches to  
23 privacy protection and could help shed light on the  
24 effectiveness of different approaches. We saw research  
25 to understand the impact of incentives and approaches to

316

1 cyber security.

2 We also saw that many of the researchers who  
3 spoke here had developed some tools that had been very  
4 useful in their own research, and many of them had  
5 actually offered to make their tools available to other  
6 researchers who could also use them. And I think the  
7 community is developing a tremendous tool set that  
8 should enable a lot more research to happen going  
9 forward.

10 We also heard from research an eagerness to  
11 partner with companies to do empirical research. Some  
12 people noted that in order to do the research they  
13 wanted to do, they needed information that only the  
14 companies have, and so there was an invitation to  
15 partner with them.

16 So, those were kind of the highlights of what  
17 I heard today. I'll be very interested in hearing from  
18 all of you about what you found useful. We're also  
19 interested in getting feedback on this event. Should we  
20 do it again? If so, should we do it exactly the same  
21 way? What should we do differently? We would be very  
22 interested in hearing that from you.

23 One of the things that I would like to do  
24 while I'm at the FTC is to try to better bridge the gap  
25 between academic research and policymakers. And I think

317

1 the privacy area is an area where there's a real need to  
 2 inform policymaking with research. And, so, as such, I  
 3 look forward to continuing the discussions that we  
 4 started here throughout the year.

5 Thank you.  
 6 (Applause.)  
 7 (Whereupon, at 5:43 p.m., the workshop was  
 8 concluded.)

9  
 10  
 11  
 12  
 13  
 14  
 15  
 16  
 17  
 18  
 19  
 20  
 21  
 22  
 23  
 24  
 25

318

1 CERTIFICATION OF REPORTER

2  
 3 CASE TITLE: PRIVACYCON WORKSHOP  
 4 DATE: JANUARY 14, 2016

5  
 6 I HEREBY CERTIFY that the transcript contained  
 7 herein is a full and accurate transcript of the notes  
 8 taken by me at the hearing on the above cause before the  
 9 FEDERAL TRADE COMMISSION to the best of my knowledge and  
 10 belief.

11  
 12 DATED: 1/20/16

13  
 14  
 15 SALLY JO QUADE

16  
 17 CERTIFICATION OF PROOFREADER

18  
 19 I HEREBY CERTIFY that I proofread the  
 20 transcript for accuracy in spelling, hyphenation,  
 21 punctuation and format.

22  
 23  
 24 SARA VANCE  
 25

<b>A</b>	50:18 51:14 55:2	142:24 186:10	147:9	<b>Adblock</b> 26:20
<b>Aaron</b> 250:8 298:8 298:14	<b>accented</b> 238:17	<b>accountable</b> 145:20 151:6	<b>activities</b> 15:16 282:9	29:10 30:4 53:15
<b>Abe's</b> 52:8	<b>accents</b> 238:20	<b>accountant</b> 178:20	<b>activity</b> 3:25 102:6 155:9 193:5,23 195:25 225:8 252:4 253:25	<b>add</b> 28:17 78:18 122:5 173:12 174:16 176:9 184:24 238:19 239:7 240:12 246:12 248:21 297:21
<b>abilities</b> 69:19 70:1 71:22 72:6,9	<b>Accenture</b> 42:19	<b>accounts</b> 152:16,20 153:4,9,10,10,12 153:16,17,22,22 154:2 155:3,5,5,13 155:17 157:16,17 157:17 175:4	<b>actor's</b> 172:7	<b>added</b> 25:8 28:25 103:14
<b>ability</b> 19:6 58:15 66:3,4 75:1 131:13 182:4 217:21 267:13 310:1	<b>accept</b> 46:10,17,24 47:7,8,9,9,16 48:11 50:14	<b>accurate</b> 277:12,23 318:7	<b>acts</b> 225:5	<b>adding</b> 123:11 248:14
<b>able</b> 15:9 20:20 25:13 28:9,16 29:12 31:2 32:5 56:13 58:17 61:19 64:7,10,24,25 93:22 103:20 114:6,7 145:23 164:6 167:17 170:17 211:22 212:25 240:8 251:25 265:7 281:20 283:2 285:7 288:10,12 288:13,18 289:7 293:4,15 294:10 304:9 306:17 307:20 310:3,8	<b>acceptable</b> 12:9	<b>achieve</b> 9:20 175:15 264:2 308:18	<b>actual</b> 74:10 87:23 88:21 95:13,19 103:8,17,20 105:16 118:15 165:23 168:20 200:15 290:6,12	<b>addition</b> 84:14 124:18 134:16 184:23 233:4 247:16
<b>absolutely</b> 150:8 183:9 184:16,22 218:10 220:2 221:14 252:20	<b>access</b> 25:10 28:9 41:21 52:23 63:24 69:5 70:24 72:14 72:22 73:2,18 74:6 77:23,25 78:4 112:8 137:4 143:21 145:22 146:2 147:13,14 150:10 165:15,18 172:20,21 176:10 181:2,25 182:12 182:13 264:17,21 265:3,10,20 279:6 284:12 287:2 306:14	<b>achieving</b> 147:16 307:1	<b>ad</b> 40:20 44:20 66:15 136:19 137:23 138:3,5,14 138:15,17,25 139:4,22,23 140:17 141:10,11 142:2,20 144:2,2,6 144:19 145:1,8,12 148:20,21,25 149:2,4 153:1,21 155:24 157:10,15 157:20,24 158:14 158:20,22 177:16 178:8,23 179:11 179:23,25 180:5 181:13 182:24 184:4,12 200:21 202:1,6,13,14 203:19 208:23 261:5,5,5,7,21 262:4,6 264:6,10 264:10 266:14 267:8,10,10,12 268:4,11,13,21 269:12 270:1,11 270:12 297:7 305:22,22	<b>additional</b> 97:21 99:1 145:21 146:4 147:13,14 184:16 184:21 195:19 198:3 278:16 299:17 311:16
<b>absorb</b> 314:13	<b>accessed</b> 73:8 74:19 75:5 76:1,8	<b>acknowledge</b> 126:5 151:14	<b>address</b> 9:23 12:17 106:21 125:3 134:6 155:1 201:7 202:7 237:6 309:15 311:22	<b>addressed</b> 12:20 63:4 111:20 303:22
<b>abstractly</b> 65:23	<b>accesses</b> 28:20 76:12	<b>acknowledged</b> 283:12	<b>addresses</b> 85:11 154:16	<b>addressing</b> 5:3 11:19 119:11 200:25
<b>abuse</b> 71:21 141:14 147:6,6	<b>accessible</b> 30:11 311:22	<b>Acquisti</b> 44:10 199:6,7 208:19 236:8 240:12 243:12	<b>adds</b> 28:7 72:16 154:6	<b>AddThis</b> 21:16 22:3 22:22 23:2,14,16
<b>abused</b> 67:1	<b>accessing</b> 74:2 75:14 112:14	<b>act</b> 40:3 89:16,18 207:9 225:16 244:21,24 282:18	<b>adequate</b> 122:25	<b>adequately</b> 192:11
<b>abuses</b> 55:22 56:20 65:20 150:19	<b>accomplish</b> 55:10	<b>acting</b> 4:20 57:9 300:13	<b>AdFisher</b> 136:24 139:3,5,7 140:25 146:13 156:16 166:1 173:22 175:3	
<b>academia</b> 26:8	<b>account</b> 64:3 84:7 86:19 123:14 148:11,16 153:3 153:18 155:8,25 174:20 201:14 248:9 253:12,14 301:18	<b>action</b> 9:6 34:14 64:12 105:11 135:11 213:13,16 226:10,10 228:17 252:25 313:4		
<b>academic</b> 6:24 7:7 11:11 38:22,23 39:5,6 177:7 236:5 302:8 316:25	<b>academically</b> 35:9	<b>actionable</b> 274:13 280:25		
<b>academics</b> 8:2 39:21	<b>accountability</b> 62:8 63:25 64:4,12,15 64:20 65:8 67:7	<b>actions</b> 9:17 39:25 64:13 151:6 182:21 213:5 220:9 228:6,7,8,10 228:10,11 245:5	<b>ad-supported</b> 262:10	
		<b>active</b> 33:13,17	<b>ad1</b> 153:5,6,17,21 <b>adapt</b> 309:14 <b>adaptive</b> 170:16	

<b>adhere</b> 98:2	<b>advantages</b> 198:9	264:14,16,24,25	207:2	<b>algorithmic</b> 315:16
<b>adjectives</b> 57:8	<b>advertise</b> 180:21	266:16 268:19	<b>agnostic</b> 154:21	<b>algorithms</b> 2:13
<b>adjust</b> 168:22	201:24 202:23	269:22 270:22	<b>ago</b> 35:16 43:22	12:18 133:24
<b>admire</b> 270:7	209:10	271:10,14 286:17	56:3 63:19 69:16	136:2 160:2 172:1
<b>admiring</b> 237:23	<b>advertisement</b>	287:4	72:11 127:8	172:13 174:12
<b>admission</b> 169:14	201:22 202:9,12	<b>Advisen</b> 223:22	222:15	309:7 315:14,17
<b>admissions</b> 169:8	202:17 203:22	225:14	<b>agree</b> 41:23 45:24	315:19,20
<b>admit</b> 169:10	204:1,2 206:16	<b>advisor</b> 123:17	45:24 48:13 59:17	<b>align</b> 11:23 98:20
<b>admitted</b> 169:15,24	243:3	<b>advocate</b> 57:7 130:5	60:20,21 107:2	99:25
<b>AdMob</b> 269:22	<b>advertisement's</b>	170:22	174:8 181:10	<b>aligned</b> 57:6 207:5
271:13	203:6	<b>advocates</b> 8:3 51:14	184:25 238:20	244:17 249:4
<b>ado</b> 68:15	<b>advertisements</b>	55:1	276:15 277:10	<b>alignment</b> 280:11
<b>adopt</b> 99:24 125:6	138:19 181:17	<b>advocating</b> 290:3	306:5,25	<b>alive</b> 235:22
222:25 223:1,7	201:18 202:3	<b>Affairs</b> 234:7	<b>agreed</b> 45:21,22	<b>ALJ's</b> 300:15
<b>adopted</b> 290:21	203:3 204:19	<b>affect</b> 149:21 150:12	46:18	<b>allegations</b> 228:12
291:7,8	205:23	210:25 239:1	<b>agreement</b> 45:23	228:13,25
<b>adopter</b> 60:1 103:18	<b>advertiser</b> 143:23	297:6	64:22 70:14 94:12	<b>alleged</b> 9:7,10
<b>adoption</b> 243:1	143:24 181:24	<b>affiliates</b> 110:3	277:7,14	<b>alleviate</b> 294:14
273:22	202:11 206:14	<b>affirmative</b> 34:13	<b>ahead</b> 48:2 85:21	<b>allocated</b> 209:12,14
<b>ads</b> 40:2 47:4 59:16	234:16 261:4,6	<b>afield</b> 240:25	88:16 94:1,2,15	<b>allocation</b> 201:4
137:1,11,15,24	263:2,6	<b>Afraid</b> 258:2	99:24 219:20	207:15 234:14
139:23 140:19,20	<b>advertiser's</b> 205:2	<b>African</b> 161:2	237:20 245:6	<b>allocative</b> 199:14
140:23 141:3,17	<b>advertisers</b> 42:11	<b>afternoon</b> 130:1,13	<b>aid</b> 11:7 13:8	<b>allow</b> 56:3 69:20
141:20 143:12	44:14 61:18 92:4	199:7 282:24	<b>aim</b> 6:23 7:8 11:11	80:23 86:14 87:4,5
144:24 146:18	97:2 139:14	<b>age</b> 43:12 49:21,22	96:15 250:11,16	99:21 112:8
147:7 148:6,15,17	140:23 144:21,23	56:6 81:15 86:13	252:2	113:14 132:8
148:17 149:10	179:9,12 201:23	91:11,16,17,17	<b>aimed</b> 170:8	184:7 265:4
151:23,24 152:6	202:8,21,22	93:11 124:12	<b>aiming</b> 293:23	273:13 279:25
152:15,22 153:2	203:24 204:7	127:20 138:7	<b>akin</b> 122:1	285:3 306:9
153:15 154:3,13	206:18 234:13	144:10 167:22	<b>al</b> 169:20	<b>allowed</b> 4:7 84:13
155:10 157:12,19	261:4 263:15,19	168:4,16 199:22	<b>Alan</b> 31:12 33:1	112:5 202:17
157:20 158:1,2,7	287:25 305:23	<b>agencies</b> 15:19	39:2 60:5 110:15	203:25 241:13
158:11,18,18,18	<b>advertising</b> 16:3	57:24 184:19	<b>alarm</b> 3:21	<b>allowing</b> 42:11
158:23 159:8	20:15 39:24 40:1	228:2 230:12	<b>album</b> 90:13	123:25 138:18
171:11 179:13,16	43:15 97:25	<b>agency</b> 7:18 55:6	<b>Aleecia</b> 44:8	313:25
179:21 181:25	143:25 181:3	118:9,9,12	<b>alert</b> 4:1	<b>allows</b> 9:25 28:19
184:11 261:17	184:1 199:15	<b>agency's</b> 5:12	<b>Alessandro</b> 44:10	109:6 138:8 139:3
262:5,12,14 263:1	200:19,20 201:9	<b>agenda</b> 5:6 6:25	199:6 200:23	140:1 146:23
263:2,16 264:21	201:15 203:9	130:25 159:5	201:2 208:17	191:1 212:14
265:4,17,17,24	209:18 211:3,13	200:13 210:6	210:16 234:12	224:9 266:18
266:5 270:24,24	235:11 241:20	300:11 312:16,18	236:6 238:16	275:14 282:17
<b>AdSDK</b> 271:16	260:22,23 261:1	<b>agent</b> 203:5	239:11 242:19	<b>alluded</b> 51:19
<b>advancement</b> 13:4	261:14,18,19,20	<b>agents</b> 202:23	<b>Alessandro's</b> 235:25	104:13
<b>advances</b> 52:19	261:23,24 262:2,3	<b>ages</b> 95:23	<b>Alexa</b> 192:10	<b>alluding</b> 42:17
<b>advancing</b> 236:5	262:8,11,15,25	<b>aggregate</b> 227:19	<b>algorithm</b> 159:16	304:7
<b>advantage</b> 70:5	263:4,8,8,9,22,24	237:15	165:7 166:6	<b>Altaweel</b> 15:12,14
111:16 220:22	263:24,25 264:8	<b>aggressively</b> 14:23	172:14,21	15:15

<b>altered</b> 108:24	307:5,6	<b>Android</b> 57:14	<b>anti-technology</b>	<b>appearance</b> 95:3
<b>alternative</b> 44:3	<b>amounts</b> 107:15	68:19 69:1,2,16	59:24	<b>appeared</b> 16:3 95:3
62:4,12 218:5	144:25 149:25	72:12 73:10 75:25	<b>anticipating</b> 243:24	<b>appears</b> 72:18,24
<b>alternatives</b> 55:7	191:15 204:8	125:25 264:22	<b>antidepressants</b>	76:2,7,14 96:17
281:11	<b>analogy</b> 114:4	265:8,9 269:23	137:25	153:21
<b>altogether</b> 243:19	116:21 131:22	270:23 271:14	<b>antsy</b> 58:19	<b>applause</b> 5:15 13:22
<b>ALVA</b> 250:3 260:18	<b>analyses</b> 47:18	289:5,6 295:1	<b>Anupam</b> 136:16,17	19:25 31:9 40:25
271:25 282:21	<b>analysis</b> 6:15 24:12	<b>Angelina</b> 213:4,7	136:23 141:22	51:23 67:20 80:10
296:25 301:19	28:1 29:1,18 31:3	<b>angle</b> 199:16	147:19 172:3	89:4 100:3 110:11
303:13 309:15	47:23 48:1 49:18	<b>angry</b> 52:4	181:13 185:1	129:2 130:21,22
312:14,25 313:19	94:17 139:2 154:7	<b>animal</b> 99:16	<b>Anupam's</b> 177:10	135:22 147:18
<b>Alzheimer's</b> 158:18	154:22 160:4	<b>Annenberg</b> 41:22	<b>anxiety</b> 267:1,17	159:14 171:4
158:19	170:15,16 184:16	<b>annotate</b> 276:9	<b>anybody</b> 251:24	186:24 199:3
<b>Amalia</b> 210:24	193:19 197:14	<b>annotated</b> 276:11	253:14,18 254:10	210:14 222:2
<b>amassed</b> 225:18	200:1 224:9 227:9	276:12 279:21	<b>anymore</b> 271:18	233:24 249:14
<b>amazing</b> 38:12	240:8 246:25	<b>annotating</b> 282:2,3	309:10	260:17 271:24
311:14	252:11 269:21	<b>annotation</b> 275:14	<b>anyway</b> 48:7 49:24	282:20 296:24
<b>Amazon</b> 152:6	274:7 275:1	275:25 276:5	58:22 64:9 117:18	314:6,7 317:6
252:13 255:2	278:17 280:20	279:14,19	119:8 253:23	<b>Apple</b> 57:19
257:7 276:8	281:9,25 282:8	<b>annotations</b> 85:7	298:12	<b>appliances</b> 6:1
280:12	303:1 306:13	280:20	<b>apart</b> 250:24 251:4	<b>applicable</b> 124:13
<b>Amazon.com</b> 252:7	<b>analysts</b> 225:14	<b>annotators</b> 84:24	253:7 255:11	151:19 152:4
<b>ambiguity</b> 275:12	240:24	275:15,25 276:10	<b>apathetic</b> 93:15	159:6
<b>ambitious</b> 6:25	<b>analytic</b> 302:22	277:4,17 278:8,14	<b>API</b> 255:22	<b>applicant</b> 169:22
295:24	303:1 308:1	<b>announced</b> 9:6	<b>APIs</b> 295:9 296:11	<b>application</b> 69:5,8
<b>Amendment</b> 64:21	<b>analytics</b> 8:18,25	<b>announcing</b> 211:23	296:14,20 304:8	69:10,19,20 70:2,4
65:7	19:7 20:16 43:11	<b>annoyed</b> 49:2	305:11 306:12	70:12,15,19,24
<b>America</b> 1:1 87:12	133:19 134:5	<b>anonymous</b> 92:14	307:3,5	71:5,21 72:7,14,22
87:24 88:11 99:20	142:19 171:21	<b>answer</b> 13:10 16:10	<b>app</b> 111:24 127:9	73:12,22,23 74:4
<b>American</b> 38:24	<b>analyze</b> 16:9 19:22	35:1,4,5 80:24	260:24 262:1,5,24	74:24 75:5,14,17
103:12 104:14	135:9 153:18	105:21 110:24	267:2,9,9,11,18,19	76:9,12,24 78:9,10
108:16,16 161:2	204:25 207:15	123:15 142:18	267:22 268:3,12	78:15,21,23
233:6	239:22 240:1	150:14 210:3	268:13,16,18,21	160:20,22 162:7
<b>Americans</b> 12:1,4	275:2,13 277:22	238:4 244:13	269:6,12 283:22	163:6,7,10,11,12
34:2,16 38:3,7,14	281:22	261:11 267:20,22	283:24,25 285:10	163:23 164:14,21
41:8,13 42:8 47:3	<b>analyzed</b> 104:17	268:1 275:18,19	285:10 286:15	165:7,8,21 166:8
49:25 50:8 104:17	274:3	275:21 277:18,20	287:5 288:9	166:18,20 167:1
<b>Amici</b> 64:6	<b>analyzing</b> 133:14	307:18	311:13 313:12	167:17,21 168:21
<b>amount</b> 17:11 46:3	274:1 276:6	<b>answered</b> 37:6 85:1	<b>apparent</b> 118:25	169:3,3,4,7,8
60:21 87:17 88:3	<b>Andelka</b> 100:7,9	<b>answering</b> 132:23	195:11 273:15	266:15,16,18
88:13 176:24	105:22 110:12	150:15	<b>apparently</b> 15:9	<b>applications</b> 69:13
177:2 180:7	111:11 112:4,16	<b>answers</b> 35:18 85:7	37:21 149:12,14	70:1 73:9,25 74:8
186:14 194:21	<b>Anderson</b> 13:19	111:10 277:15	149:15 158:23	75:20 76:15,17
195:25 201:11	68:3,5 80:11 89:5	278:7,12 290:13	261:10	77:2,4,22,24 78:16
208:1 223:8,8,9	100:4 110:12	309:8	<b>appear</b> 46:20 69:25	79:18 159:18
246:9,10,11	124:6 125:15	<b>anti-discrimination</b>	76:5 77:5,11 106:4	160:9 161:9 162:1
262:20 266:12	128:3 130:3	219:6	269:16	163:4,19 166:22

166:23,24 170:9 170:12,25 <b>applied</b> 166:22 170:11 302:7 <b>applies</b> 177:10 <b>apply</b> 162:11 164:23 169:9 236:21 302:3 <b>applying</b> 168:1 198:1 <b>appreciate</b> 249:13 283:1 <b>approach</b> 32:13 39:19 62:19 63:4 81:8 82:11,12 97:15,17 132:24 189:11,13 194:19 259:22 274:25 278:5 279:15,20 280:10 294:2 302:7,8 <b>approachable</b> 98:11 <b>approaches</b> 131:9 214:10,12 273:19 273:20 315:22,24 315:25 <b>approaching</b> 193:7 246:18 304:22 <b>appropriate</b> 144:11 223:8 298:17 <b>approves</b> 123:24 <b>approximation</b> 127:20 <b>apps</b> 51:7 60:14 112:14 260:25 262:2,7,10 265:12 265:18 269:6,24 270:3 274:3 283:8 283:17,19 284:10 284:11 286:14 289:12 290:12 291:6 292:2 296:2 296:3 305:1 306:7 <b>arbitrary</b> 152:6 <b>arc</b> 41:6 <b>architecture</b> 156:21 <b>archived</b> 4:13	<b>area</b> 3:24 65:16 95:17 104:13 115:22 141:25 142:5 146:15 147:10 210:7,7 242:15 280:7 288:8,23 292:4 301:9 317:1,1 <b>areas</b> 9:21 147:9 171:22 241:10,18 314:16,18 <b>arena</b> 242:10 <b>arenas</b> 11:14 <b>arguable</b> 124:23 <b>argue</b> 34:15 38:17 43:2 50:21 59:24 62:7 122:9 161:9 162:22 195:7 196:12,15 218:19 219:14 230:19 <b>arguing</b> 64:7 123:21 <b>argument</b> 52:17 64:19 65:7 195:4 <b>arises</b> 192:3 <b>arms</b> 309:19 <b>array</b> 7:19 11:6 <b>arrives</b> 202:5 <b>article</b> 137:24 <b>articulate</b> 55:13 211:13 <b>articulated</b> 212:6 <b>artifact</b> 229:12 <b>artists</b> 305:22 <b>Ashwini</b> 80:12 89:5 111:18,21 112:3 112:15 115:15 275:5 285:13 <b>aside</b> 130:23 181:9 <b>asked</b> 9:21 36:17 37:12 47:6,12,14 69:18 74:16 78:3 83:16 90:4,6,10,13 90:20 104:6,7,22 105:2 235:5 276:9 290:8 <b>asking</b> 34:2,22 37:2 78:20 84:8 92:1	215:3 262:13 267:15 279:2 289:9,17 296:5,8 302:15 <b>aspect</b> 51:1 155:21 156:21 <b>aspects</b> 51:11 132:19 189:19 246:16 274:11 279:8 292:10 <b>assemble</b> 3:23 <b>assembly</b> 3:24 <b>assertion</b> 41:10 <b>assertions</b> 47:22 <b>assess</b> 195:1 223:15 239:13 273:2 <b>assessing</b> 89:22 92:16 133:8 <b>assessment</b> 156:12 198:23 <b>assign</b> 97:23 <b>assigned</b> 175:4 <b>assigning</b> 143:9 147:11 <b>assignment</b> 142:25 186:11,17 <b>assigns</b> 139:10 <b>assist</b> 314:24 <b>assistant</b> 290:10,11 295:16,19 296:9 <b>assistants</b> 283:7 285:2,6,23 286:3 290:22 291:6 293:15,17,21 295:11 297:18 312:21 <b>associated</b> 162:5 192:5 194:22 <b>Associates</b> 45:6 <b>association</b> 162:19 163:25 164:2,10 164:17 165:2 168:3,8,16 169:17 169:19 <b>associations</b> 156:13 159:18 162:2,24 164:20 165:1	166:5,7 168:24 <b>associative</b> 214:12 <b>assume</b> 39:12 76:3 81:9 83:16 155:23 177:18 202:22 203:4,11 <b>assumed</b> 119:7 <b>assuming</b> 63:3 <b>assumption</b> 65:11 140:7 245:9 <b>assumptions</b> 7:3 46:25 47:10 140:5 <b>asymmetric</b> 236:20 <b>asymmetry</b> 22:16 119:22 237:7 <b>AT&amp;T</b> 176:19 <b>attached</b> 257:17 <b>attack</b> 32:8 64:11 194:11 269:11 <b>attacked</b> 227:5 <b>attacks</b> 64:3 224:19 224:25 225:6 226:19 227:11,17 <b>attempt</b> 90:9 <b>attempted</b> 91:21 92:10 <b>attempts</b> 15:24 <b>attendance</b> 40:20 <b>attention</b> 33:10,24 80:8 142:9 194:9 210:13 <b>attentive</b> 181:24 <b>attests</b> 63:15 <b>attitudinal</b> 34:6 <b>attorney</b> 68:5 <b>attribute</b> 162:18 <b>attributes</b> 161:25 162:4,6,15 164:1 164:11,13,21 166:8 293:6 <b>auction</b> 202:9,15 203:6,21,24 263:18 <b>auctions</b> 202:14 <b>audience</b> 128:9 135:13 148:23 149:6 176:4	211:24 215:25 216:8 225:1 267:23 271:21 282:25 283:14 313:20 <b>audio</b> 26:4 52:15 229:3 <b>auditing</b> 207:20 <b>auditorium</b> 4:5,8,10 128:13,16 <b>audits</b> 307:19 <b>augment</b> 79:19 <b>Augustin</b> 155:20 <b>Australia</b> 99:10,20 105:18 <b>Australian</b> 102:19 103:13 <b>Australians</b> 104:19 <b>authoring</b> 298:2 <b>authority</b> 121:15 <b>automate</b> 280:9,19 289:20 <b>automated</b> 10:2 24:2 136:19 <b>automatic</b> 54:2 124:17 <b>automatically</b> 71:17 160:24 164:3 285:8 315:2 <b>automation</b> 27:24 29:17 140:11 146:23 <b>automations</b> 154:6 <b>availability</b> 301:12 <b>available</b> 4:4,14 9:16 10:15 12:22 128:11,12 145:4 170:13 181:7,21 182:1 191:14 201:11,22 204:5,9 204:11,12,13,15 205:18 206:6,23 208:11,12 233:7 255:25 261:4 263:4,6 281:7,16 301:3 309:4 316:5 <b>average</b> 42:12 45:2
---	--	---	--	--

77:17 91:11 96:16 97:20 98:24 124:9 177:23 193:16,21 211:20 212:22 230:21 286:22 <b>avoid</b> 5:3 12:23 40:18 99:11 172:12,16,18 173:16 174:1 <b>avoiding</b> 8:18 <b>avowed</b> 121:11 <b>aware</b> 109:1 110:2 148:9 160:8 246:6 307:11 <b>awareness</b> 151:2 <b>awesome</b> 30:24 <b>AWS</b> 257:7	220:1,3,4 221:5,15 221:19 232:19,21 248:1,25 251:12 299:13 311:25 <b>badge</b> 3:16 <b>badly</b> 168:4 <b>Bain</b> 41:22 42:19,20 <b>balance</b> 193:3 302:10 308:3 <b>balls</b> 301:22 <b>Bank</b> 87:12,24 88:11 <b>banking</b> 81:11,18 87:9,10 <b>banner</b> 178:13 <b>bar</b> 76:3 216:9 277:15 <b>bargain</b> 12:8 121:20 <b>Barrett</b> 143:24 144:6,8 <b>base</b> 50:9 165:14 <b>based</b> 25:4 32:14 33:2 47:10 48:1 55:11 59:10 70:22 76:16 79:14,23,25 81:13 82:5 83:23 87:16 97:20 99:19 107:16 116:9 123:1 124:8,20 127:1 137:16 158:7 160:12 174:2 178:8 183:13 212:22 213:5 220:20 223:22 244:16 256:4 279:13 285:8,10 286:7,7 288:11,12 290:12 290:13,21 291:9 293:17 295:23 309:22 <b>baseline</b> 216:17 <b>basic</b> 12:8 34:9 35:17 37:5 49:25 110:24 <b>basically</b> 24:22 25:13 28:9 38:17	106:5 217:12 246:25 250:11,12 252:2,6,13 253:10 253:23 254:24 255:2 256:14 257:16,25 259:24 274:17 275:14,18 280:17 281:15 306:12,15 310:22 <b>basics</b> 37:4 <b>basis</b> 33:19 60:22 79:11 80:19 202:10,19 203:23 298:23 <b>basket</b> 301:22 <b>battery</b> 76:11 <b>battle</b> 33:22 <b>BBC</b> 21:25 <b>beacons</b> 52:15 <b>beam</b> 245:16 <b>bear</b> 3:12 <b>bearing</b> 225:5 231:17,18 <b>beating</b> 245:22 <b>beautiful</b> 36:15 222:17 236:15,25 238:12 <b>becoming</b> 61:3 281:4 <b>bee</b> 214:1 <b>beef</b> 116:25 120:4,7 <b>beginning</b> 51:11,12 76:23 142:1,5,8 151:25 152:23 176:13 177:1 185:2,4 <b>begun</b> 50:24 97:15 111:13 <b>behalf</b> 62:15 295:13 296:12 <b>behave</b> 90:5 139:22 163:8 197:20 245:23,24 <b>behaving</b> 146:21 <b>behavior</b> 41:12 78:3 92:17 93:7 95:10 95:13,20 96:14,16	137:18 138:14 139:15 240:4 260:14 268:21,24 286:1 292:10 309:4 <b>behavioral</b> 139:1 199:10,16,17 240:1 <b>behaviors</b> 79:15 91:3 139:12 <b>belief</b> 45:25 93:23 240:15 318:10 <b>believe</b> 15:16 49:5 49:15 50:4 59:5 93:24,25 120:15 150:16 197:13 198:6 199:22 209:9 210:2 241:17 243:17 244:8 249:8 283:9 289:21 292:1 294:2 304:25 312:20 <b>believes</b> 46:2 237:4 <b>believing</b> 48:19 <b>belong</b> 266:5 <b>benchmark</b> 15:20 15:21 204:14 <b>beneficial</b> 122:19 150:7 299:14 <b>benefit</b> 11:13 42:10 50:1 111:7 113:2 119:8 199:25 234:15 247:5 296:20 304:14 305:10 <b>benefits</b> 6:11 8:9,18 12:12 41:9 49:16 50:8 112:19,22 198:11 200:9,11 201:4 207:16 208:2 209:11 210:1 234:14 247:3,4 299:23 <b>Berkeley</b> 15:12 31:20 68:18 136:17 169:9,15	171:7,17 <b>best</b> 112:21 113:3 198:9 204:17 208:3,7 220:15 304:25 318:9 <b>bet</b> 149:21 <b>Beth</b> 15:18 <b>better</b> 11:21 58:10 89:1 96:15 113:19 119:15 123:7 125:14,14 131:22 133:15 138:21 170:23,24 180:22 189:5 195:22 197:14 205:14,17 205:24 206:3 207:13,24 208:5,9 224:10 230:22 239:8 244:13 274:18,23 285:3 292:24 304:14 305:13,13 310:15 316:24 <b>beverages</b> 128:16 <b>beyond</b> 23:9 26:8 29:7 66:5 133:9,18 174:16 281:12 <b>bias</b> 12:20 169:14 172:5,14,15 <b>biased</b> 313:18 <b>biases</b> 8:21 70:20 171:24,25 172:13 299:13 <b>Bickel</b> 169:20 <b>bid</b> 144:1,25 202:11 202:13,16,16 203:24 206:15,18 207:2 <b>bidder</b> 202:15 <b>bidders</b> 207:1 <b>bidding</b> 182:3 201:16,17 <b>big</b> 2:13 8:15,17,25 12:18,20 23:5 31:23 43:5 52:12 63:13 94:18 133:18,21 134:5
<b>B</b>				
<b>B</b> 238:5 <b>back</b> 3:11 21:4 27:21 29:3 30:21 38:13 43:8 58:11 67:18 74:13 91:4 105:13 116:3 122:10 128:18,20 128:24,25 136:5 137:14 172:6 174:11 186:23 188:3 209:1 220:10 231:6 236:16 243:12 251:10 285:12 302:5 303:12 306:10 <b>backed</b> 123:23 <b>backfires</b> 309:14 <b>background</b> 32:23 47:15 73:24 75:21 78:17,23 124:11 216:3 257:11 <b>bad</b> 66:13 123:4 127:6 150:11 168:5 172:16 173:7 174:1 182:9 182:14 183:12 210:4 219:25				

136:2 147:8 150:7	258:17	226:22 228:22	152:4 159:6	27:25 31:2 150:23
159:15 170:15	<b>blocked</b> 10:17 29:10	229:5,13,14	298:12	157:7 245:7
174:24 175:13,13	78:5	239:23	<b>broke</b> 103:16	275:21 296:18
176:1 180:18	<b>blog</b> 246:22	<b>break</b> 67:18 90:13	<b>broken</b> 91:12	313:13
216:10,23 230:13	<b>blossomed</b> 63:17	186:21 279:17	224:13	<b>builders</b> 305:23
243:1 244:20,21	<b>blue</b> 178:19 207:23	<b>breakdown</b> 91:15	<b>brokers</b> 7:25 149:12	<b>building</b> 3:10,18,21
247:22 251:4	<b>bluetooth</b> 257:18	91:18	<b>Brookman</b> 14:3,6	3:22 4:1,3 25:6
252:1 256:12	<b>blunt</b> 312:8,8,12	<b>breakdowns</b> 91:6	20:1 31:10 41:1	30:7 112:25
257:3 258:5 259:1	<b>board</b> 184:22	<b>breakthroughs</b> 13:7	51:24 56:25 62:2	128:17 132:2
260:23 262:23	<b>body</b> 146:13 186:12	<b>breast</b> 109:23	63:6 66:8 67:14,16	135:2 148:2 151:8
263:7 271:21	<b>bold</b> 33:12	213:10 215:9	<b>brought</b> 8:2 139:25	159:5 175:20
298:2 301:22	<b>Bond</b> 42:19	<b>brick-and-mortar</b>	180:13 181:13	184:6,17 185:2
303:1 306:6	<b>bonnet</b> 214:2	183:5	228:10,11,17	258:15,17 275:14
311:21 314:6	<b>book</b> 38:24 40:18,21	<b>bridge</b> 6:23 95:20	302:21	292:8,22,25 294:3
<b>bigger</b> 122:22	298:2	316:24	<b>browse</b> 5:24 25:23	294:12 295:20
<b>biggest</b> 112:19	<b>boost</b> 216:23	<b>brief</b> 3:6 52:1 68:25	139:9 140:17	296:17 307:16
174:24 220:21	<b>borders</b> 108:19	110:20 183:25,25	<b>browsed</b> 18:18	<b>builds</b> 10:24 11:10
271:13 283:21	<b>boring</b> 36:12	184:25 314:3	<b>browser</b> 17:6 18:5	52:25
<b>binary</b> 210:3	<b>bother</b> 271:18	<b>briefly</b> 7:14 123:16	21:10,11 24:9,22	<b>built</b> 13:6 24:16
<b>bio</b> 178:20	<b>bottom</b> 96:8	234:3	25:1,11,12,14	25:8 26:24 75:24
<b>biobank</b> 102:23	<b>bought</b> 42:21 252:6	<b>briefs</b> 64:6	26:17,20 28:8	151:13 157:5,6,10
<b>biometrics</b> 107:20	<b>bound</b> 122:2	<b>brightest</b> 112:21	82:19 139:8 154:6	157:23 202:19
<b>bit</b> 24:15 26:9 89:24	<b>bounties</b> 188:15	283:23	261:20,21 264:7,8	286:13
90:4 91:14 93:3,14	190:4 193:9,13,14	<b>Brill</b> 2:5 12:25 130:4	264:9 269:7,17	<b>bulk</b> 5:3 228:9
93:15 120:10	194:17 258:25	130:5,8,9,23	281:15 294:22,24	<b>bunch</b> 21:17,22
122:10 124:7	259:1,3	135:23 136:3	296:4	22:18 24:8 26:18
131:21 140:16	<b>bounty</b> 188:18,23	<b>Brill's</b> 235:24	<b>browser's</b> 21:11	27:12,15,15,25
150:17 152:25	190:22 191:15	<b>bring</b> 134:4 146:23	<b>browsers</b> 17:7 25:17	29:6 32:25 37:1
164:18 165:5	193:21 194:2,21	213:3 305:7	264:13 271:3	139:7 148:12
191:13 195:21	198:22 234:9	<b>bringing</b> 5:20 303:7	<b>browsewrap</b> 121:25	157:6 158:3 185:6
215:17 222:12	246:14,19,24	304:4,11	<b>browsing</b> 20:9 30:2	220:17 250:13
231:9,15,22	247:8,13 248:12	<b>brings</b> 112:20 121:9	138:14 147:4,6	<b>burden</b> 89:1 285:3
236:16 242:7	259:9	146:14 194:24	176:22	294:14
261:16,18 266:6,6	<b>boxed</b> 4:4 128:11	197:12 198:25	<b>bucket</b> 214:4 216:10	<b>Bureau</b> 68:7
272:19 276:23	<b>brand</b> 42:19 57:21	257:24	<b>buckets</b> 214:5	<b>burrito</b> 114:5,9,15
289:1 298:12,19	63:13	<b>broad</b> 110:2 134:4	<b>budget</b> 179:9	114:18,23 116:21
301:24	<b>Brandeis</b> 54:9	189:13 190:13	<b>bug</b> 164:6,22 188:15	<b>burritos</b> 131:22
<b>black-hat</b> 196:25	<b>brands</b> 57:21 92:3	191:10 209:8	188:18,23 189:6	<b>bus</b> 58:18 117:20,23
240:9	206:5	<b>broadcasted</b> 202:6	234:9 246:14,19	118:2
<b>black-hats</b> 189:14	<b>brave</b> 105:11	<b>broader</b> 11:6 45:23	246:24 247:1,8,13	<b>business</b> 57:5 98:1
240:4	<b>breach</b> 101:8 226:5	45:25 49:11 62:3	248:12 256:19	119:25 180:4
<b>black-hatted</b> 247:20	228:15 229:15	65:12 100:23	258:24 259:1,3,9	263:13
<b>blackbox</b> 140:1	230:4,14,18,23,24	103:4 184:8	259:10	<b>businesses</b> 8:6,17
<b>blaming</b> 56:13	230:25 231:4	190:19 191:1	<b>bugs</b> 161:10,12,15	55:24 97:1 113:19
<b>blindness</b> 107:1	233:8,10 240:21	200:13 209:1	161:15,18 162:23	297:14
<b>blissfully</b> 58:10	<b>breaches</b> 224:7,17	<b>broadly</b> 105:5	258:24 259:21	<b>busy</b> 314:14
<b>block</b> 93:10,17 94:4	225:2,4 226:13,15	142:10 151:19	<b>build</b> 10:21 24:12	<b>button</b> 72:21 253:1

253:1,16,17,18 254:14,17 <b>buttons</b> 20:14 <b>buy</b> 39:11 47:11 179:14 202:24 258:6 <b>buying</b> 120:22	<b>can't</b> 62:6 307:25 <b>cancer</b> 109:24 158:24 209:19 213:10,14 215:9 220:4 <b>canvas</b> 21:7,8,15 22:4,8,13 23:3 26:24,25 27:2,15 27:15,21 28:24 29:2,2,25 30:6,8 <b>capabilities</b> 18:1 28:8 55:4 133:9 <b>capability</b> 135:10 169:5 170:5 255:19 258:10 308:1 <b>capable</b> 192:14 250:25 253:7 <b>capacities</b> 123:20 <b>capacity</b> 10:21 135:10 <b>capture</b> 208:1 305:17,18 310:8 <b>captured</b> 207:20 <b>captures</b> 205:5,7,13 205:16 206:1 <b>capturing</b> 203:13,14 <b>car</b> 117:20 160:25 <b>cards</b> 12:9 74:12 128:13 <b>care</b> 36:7 37:21 38:20 58:2,3 77:20 79:8 101:18,20,23 101:25 126:19,22 166:25 181:17 218:15 227:24 237:13 274:12 280:25 282:7,10 283:14 294:12 304:16,20 <b>cared</b> 138:9 <b>career</b> 141:3,10 143:25 178:8 <b>careful</b> 115:16 236:22 <b>carefully</b> 265:24,24 <b>careless</b> 93:15	<b>caricature</b> 163:10 <b>Carnegie</b> 80:12 136:17 199:6 272:1 282:23 313:24 <b>cars</b> 6:2 131:23,23 <b>cart</b> 119:11 <b>case</b> 24:17 26:23 30:24 64:5,5 65:12 65:19 78:3 85:21 86:2,3 88:10 90:25 93:20 94:16 117:23 118:19 119:5 143:24 145:6 153:20 160:21 167:4 172:23 196:19 204:10,12,13,14 204:15 207:18,25 207:25 208:3,6,7 217:10 241:18,18 246:5 249:2 252:3 259:25 266:22 267:15 283:22 290:7 291:12 292:18,19,19 298:16 300:16 306:16 308:7,9 310:24 318:3 <b>cases</b> 66:18 75:16,20 76:7 77:22 78:1 152:10 191:11 204:10,16 208:2 230:8 249:2,5 275:3 277:9,13 <b>catch</b> 97:24 <b>categories</b> 103:18 158:9 190:13 203:12 224:14 234:20 <b>categorize</b> 127:14 <b>categorized</b> 203:12 203:18 <b>categorizing</b> 224:15 <b>category</b> 158:16 279:3,4,9 <b>cater</b> 80:2	<b>Catherine</b> 210:16 210:20 222:3 234:18 236:24 241:5,5 <b>caught</b> 64:17 125:11 185:19 <b>causal</b> 146:16 177:19 220:16 235:20 238:6 240:20 <b>causality</b> 182:8 <b>causation</b> 152:19 <b>cause</b> 140:2 318:8 <b>caused</b> 146:17 225:5 <b>causes</b> 222:5 228:17 <b>causing</b> 71:20 224:20 <b>cautions</b> 42:20 <b>cautious</b> 12:13 <b>caveat</b> 52:1 88:15 <b>cell</b> 284:17 290:6,13 294:25 <b>cellular</b> 76:16 <b>census</b> 15:13,15,20 16:7,8 17:10 19:13 26:7 30:23 98:23 <b>center</b> 1:9 3:18 11:25 102:14 141:16,17 272:9 297:24 <b>centers</b> 134:19 <b>certain</b> 8:22,23 9:21 12:3 24:23 34:14 39:13,14 50:6 56:17 60:21,21 69:6 72:15 81:10 87:15 116:24 117:1,8 121:16 127:10 134:1 138:1 161:24 172:16 195:25 199:19 232:20 246:9 255:11 260:6 269:13 277:6 306:8 <b>certainly</b> 63:12 175:22 220:15	222:22 224:15 226:3 230:1 238:5 238:14 247:9,15 247:22 287:2 299:6 <b>certainty</b> 268:7 <b>CERTIFY</b> 318:6,19 <b>cetera</b> 60:8 93:16 94:25 98:4 102:11 <b>chain</b> 163:5,22 186:10 <b>Chaintreau</b> 155:21 <b>chair</b> 14:9 <b>Chairwoman</b> 2:4 5:11,14,16 14:4 113:5 130:16 <b>challenge</b> 10:15 41:10 148:19 155:14,15 <b>challenges</b> 6:18 10:11 135:14 154:17,25 284:19 294:20 <b>challenging</b> 154:9 154:16 305:6 <b>chance</b> 5:5 27:16 61:7 211:20 222:1 <b>chances</b> 71:22 213:14 284:23 <b>change</b> 6:17 55:19 67:7 101:8 109:6 109:11,15 116:10 126:2 139:14 184:5 201:3 233:17,22 286:6 291:12 309:9 <b>changed</b> 125:20,23 <b>changes</b> 55:19 109:10 143:4 204:7 205:2 207:16 227:2 309:4 <b>changing</b> 21:1 71:19 116:7,13 120:18 <b>channel</b> 183:4 <b>characteristics</b> 33:13 81:15 83:22
---	---	--	--	--

83:22,24 86:6,11 <b>characterize</b> 163:9 <b>Charbonneau</b> 100:8 100:12 126:4 <b>charge</b> 45:16 183:19 183:23 <b>chart</b> 52:11 207:17 207:21 216:10 239:21 286:19 287:10,12 288:22 <b>charts</b> 207:22 <b>chats</b> 256:8 <b>chatting</b> 256:5 <b>cheap</b> 10:2 <b>cheaper</b> 282:5 <b>cheater</b> 158:22 <b>cheating</b> 158:22 <b>check</b> 26:14 31:6,7 163:5,24 164:9 165:21 166:11 <b>checklist</b> 308:5 <b>checks</b> 162:11 <b>cheeseburger</b> 58:3 <b>Chicago</b> 236:14 <b>chief</b> 4:20 12:25 246:23 313:22 <b>chiefly</b> 107:9 <b>chime</b> 14:24 <b>Chinese</b> 189:2 <b>Chipotle</b> 114:5,9,14 114:23 116:22 131:21 <b>chocolate</b> 40:22 <b>choice</b> 32:13,15,16 32:24 33:2 40:7,14 42:16 51:9 52:21 54:3 55:5 69:4,12 71:10 76:23 80:7 96:22 122:23 123:1 124:2 131:10 204:20 245:20,20,21 281:1 294:5 303:5 315:5 <b>choices</b> 32:5,18 33:4 40:14 44:20 50:1,9 54:13 56:9 62:15	98:15 99:7 241:7 242:9 246:2,8 272:17 273:9 274:20 281:5,7,11 306:16 <b>choose</b> 23:25 208:15 302:25 <b>chose</b> 92:17 <b>Chris</b> 31:11 41:1 42:7,16 44:6 50:2 62:25 63:8 <b>Chris'</b> 52:17 <b>circles</b> 200:19 <b>circumstances</b> 12:3 73:3 138:1 <b>cite</b> 43:19 <b>citizen</b> 59:2 <b>civil</b> 226:10 228:11 <b>claim</b> 209:3 301:2 <b>claiming</b> 141:8 209:5,6 <b>claims</b> 47:18 120:13 213:2 226:14 228:25 <b>clarify</b> 248:23 <b>clarity</b> 56:14 <b>class</b> 64:12,13 <b>classes</b> 52:2 <b>classified</b> 191:12 <b>classifiers</b> 275:23 <b>clause</b> 109:6 <b>clauses</b> 109:20 111:13 112:17 <b>clean</b> 289:1 <b>clear</b> 56:18 85:8 115:15 138:22 172:15 198:20 225:12 252:20,24 253:2,8,13 254:6 254:18 255:9,13 255:17 256:6,17 256:23 257:6 289:23 304:18 309:18 310:23 <b>clearer</b> 112:17 308:16 <b>Clearinghouse</b>	15:19 <b>clearly</b> 57:18 63:10 105:8 255:18 286:23 287:21 303:25 304:8 312:21 <b>clever</b> 96:24 166:6 238:10 <b>click</b> 10:3 70:14 90:23 92:16,18 94:2,11 107:2 118:21 150:2 163:18 178:1 <b>click-down</b> 178:19 <b>click-through</b> 177:21 <b>clicked</b> 217:8 <b>clicking</b> 72:21 93:6 93:13,23 95:7,9 145:8 <b>clicks</b> 70:17 179:23 <b>clickthrough</b> 145:11 <b>clinics</b> 134:19 <b>clock</b> 14:23 <b>close</b> 13:13 98:23 235:8 289:18 291:24 <b>closely</b> 248:3 <b>closer</b> 13:12 46:12 135:3 180:22 <b>closing</b> 67:14 119:22 170:10 <b>cloud</b> 251:7,9,14 252:5 <b>CMU</b> 272:8 308:24 <b>co-author</b> 15:15 19:24 <b>co-authors</b> 27:11,13 174:10 <b>co-discussants</b> 15:5 54:7 110:15 113:13 <b>co-panelists</b> 14:11 <b>co-presenters</b> 89:6 100:6 <b>co-presenting</b> 14:8 <b>co-significance</b>	140:4 <b>coaching</b> 141:3,10 143:25 <b>coarse</b> 286:25 <b>code</b> 28:1,25 29:1,19 30:15 137:12,13 137:14,20 139:1 262:4,4,6 306:14 <b>coded</b> 34:17 <b>coerce</b> 193:4 <b>coerced</b> 190:20 192:25 196:7 <b>cognitive</b> 70:19 123:17 <b>cognizant</b> 43:21 <b>coin</b> 78:13 <b>coincidentally</b> 135:11 <b>Coke</b> 179:13,14 <b>Coli</b> 120:4,7 <b>collaborate</b> 30:16 31:7 <b>collaboration</b> 108:20 143:2,7 176:12 272:8 <b>collaborative</b> 172:4 <b>collaborator</b> 155:20 <b>collaborators</b> 151:15 159:23 176:5,19 <b>collar</b> 178:19 <b>colleague</b> 12:24 115:20 237:23 <b>colleagues</b> 233:5 <b>colleagues'</b> 115:15 <b>collect</b> 16:8 17:14 19:21 45:11 53:25 80:22 81:11,12,18 84:9,14,15 85:18 85:24 86:18 87:9 87:13 92:23 97:1 98:21 132:17 139:14 149:25 153:15 157:18 176:21 237:11 292:17,20 293:6 <b>collected</b> 12:15	16:19 18:17 66:2 73:19 76:4,20 77:7 87:5 111:3 119:1 131:18 136:6 140:18 171:10 276:4 283:18 305:14 <b>collecting</b> 26:11 46:9 85:19 86:1 98:1 107:14 125:1 154:3 165:10 246:7 279:20 284:1 293:2 307:4 <b>collection</b> 16:19 17:4 38:4,6 41:8 43:4 50:6 66:4,5 66:10,11,13,14,24 67:4 81:2 84:1,2,6 86:17 97:18,22 111:19 112:12 124:22,24 200:1,7 224:24 225:19 276:20 279:5 280:13,16 305:20 306:2 <b>collective</b> 54:25 <b>collects</b> 50:15 85:2 157:20 <b>college</b> 117:15 188:13 <b>colors</b> 205:11,15 <b>Columbia</b> 147:21 148:2 150:20 159:17,22 <b>combination</b> 135:10 146:24 153:6 206:9,20 209:15 251:12,15 275:21 <b>combinations</b> 155:12,13 205:16 206:2 <b>combined</b> 106:10 210:8 <b>combining</b> 191:17 274:5 <b>Comcast</b> 19:12 <b>come</b> 3:11 9:22 13:4
--	--	---	---	--

34:1 39:22 40:3 43:14 48:11 62:3 64:15 67:18 69:22 87:17 92:25 93:18 101:9 113:16 115:13 119:17 124:20 127:24 128:18,20 135:19 136:4 144:24 160:8 167:12 184:17,18 211:16 220:16 225:12 230:17 232:23 237:15,16 245:5 258:6,18 271:22 275:3 277:8,11,16 278:14 287:17 288:1 291:18 295:22 304:18 308:18 312:13 <b>comes</b> 39:19 102:23 116:4 117:25 134:12 148:22 161:16 163:1,21 169:19 197:5 198:16 223:21 231:15 239:16 273:25 286:22 287:1,11,13 290:25 291:1 295:22 296:2,17 305:2 306:10 <b>comfortable</b> 121:8 287:20 309:13 <b>coming</b> 14:5 31:4 58:22 61:1 113:11 120:20 124:8 126:12 128:25 138:19 166:15 185:9 213:22 217:4 225:11 238:11 250:22 256:11 257:4,20 258:21 259:2 314:10 <b>commence</b> 3:6 <b>comment</b> 61:2 177:7	177:8 178:4 183:25 184:15 236:8 309:18 <b>comments</b> 62:20 110:20 116:20 184:23 235:24 301:7 <b>commercial</b> 12:2 16:2 102:4,21 103:1 105:17 <b>commercialization</b> 126:6 <b>commercializing</b> 126:22 <b>Commission</b> 1:2,8 5:20 31:14 39:20 39:21,25 97:7 151:4 188:5 234:5 318:9 <b>Commission's</b> 39:23 108:15 <b>Commissioner</b> 2:5 12:25 66:20 130:4 130:5,8,9,23 135:23 136:3 235:24 <b>commitments</b> 134:13 <b>committed</b> 70:18 <b>common</b> 46:2 68:13 109:4 111:9 171:14 174:7,9 189:19 200:4 209:4 228:13 252:16 254:3 262:7 305:5,9 <b>Commonly</b> 202:13 <b>communicate</b> 132:12 201:25 308:23 <b>communicated</b> 190:9 <b>communicating</b> 308:23 <b>communication</b> 25:1 311:23 <b>communications</b>	132:9,11 150:17 <b>communities</b> 7:8 11:12 105:15 <b>community</b> 6:20 142:10 146:8,25 160:1 240:10 248:16 298:2 316:7 <b>commute</b> 100:9 <b>compact</b> 279:11 <b>companies</b> 5:22 9:4 12:15 16:15 18:21 19:10,19 20:15,16 21:17 22:19 32:7 40:13 42:14,21 43:7 45:10 52:10 52:12 55:18 58:24 60:14 62:5,8 65:2 67:11 92:22,22 103:6 105:8,19 106:1 107:13 108:16 109:5,5,11 109:14,19 111:13 112:11 131:19,24 132:1,7,16,17,21 133:23 134:3 137:21 138:3 146:9 149:15 176:11 189:17,24 190:18,19 191:6 192:5,9,25 193:4 193:11,12 196:17 196:18,19 201:5 201:24 205:25 216:21 223:23 231:3 232:15 237:14 247:11 248:18 271:10 273:12,22 295:17 300:4,9 310:9,14 310:17 316:11,14 <b>companies'</b> 11:23 12:21 55:23 112:1 112:5 <b>company</b> 41:22 62:10 106:13 111:15 120:22	123:10 167:3,4 181:19 185:17 190:7 196:8 223:21 224:20,20 247:10 257:3 263:10 <b>company's</b> 9:7 66:7 <b>company-initiated</b> 192:19 198:8 <b>company-sponsor...</b> 188:21 <b>compare</b> 58:16 86:22 88:20,21 176:23 190:12 201:10 276:4 280:13 <b>compared</b> 27:8 49:14 83:8,20 152:2 178:16 277:3 <b>comparing</b> 79:3 <b>comparison</b> 70:21 190:14 <b>compatible</b> 60:4 <b>compensation</b> 42:22 194:14 <b>competition</b> 7:20 11:8 121:15 167:5 167:16 183:15 204:25 207:1 248:16 299:4 <b>compile</b> 163:7 <b>complain</b> 22:20 23:21,23 <b>complaining</b> 23:1,7 <b>complaints</b> 89:22 126:15 <b>complementary</b> 82:12 <b>complete</b> 181:22 186:4,10 208:6 278:3 279:11 <b>completely</b> 73:3 75:18 161:24 183:3 184:25 257:10 <b>complex</b> 6:3 13:9	58:1 79:16 121:5 131:20 140:7 150:9 152:13 194:9 270:8 273:7 277:25 278:23 287:15,22 <b>complexities</b> 142:19 <b>complexity</b> 6:17 52:8 131:25 <b>compliance</b> 272:25 273:3 308:4 <b>complicated</b> 58:14 145:19 276:23 <b>complication</b> 116:4 <b>complications</b> 115:13 <b>comply</b> 105:20 <b>component</b> 29:20 <b>compounds</b> 155:10 <b>comprehensive</b> 270:22 <b>compressed</b> 156:2 <b>compromises</b> 239:10 <b>computer</b> 32:9 44:6 68:17 131:1 133:2 134:25 143:3,5,6 250:20 271:20 282:23 302:6 311:23 <b>computers</b> 131:23 251:1 <b>computing</b> 43:21 <b>concentration</b> 16:15 18:20 <b>concept</b> 43:13 81:24 156:1 <b>concepts</b> 69:23 236:20 <b>concern</b> 41:25 81:16 92:20 95:16,19,24 96:1,5,11,13,14 97:3 <b>concerned</b> 38:4,7,14 41:20 51:13 54:10 62:25 66:9,24 127:16,25 142:4
--	--	---	--	--

173:4 179:20,22 181:5,8 242:15 246:11 282:10 <b>concerning</b> 73:5 108:22 109:3 137:22 140:24 141:12,18 308:11 <b>concerns</b> 102:20 125:19 126:25 138:2 142:10 219:23 233:15 274:9 275:5 <b>concert</b> 309:11 <b>concise</b> 98:16 123:23 <b>conclude</b> 68:11 100:2 191:21 296:25 313:21 <b>concluded</b> 69:24 71:9 234:13,20 317:8 <b>conclusion</b> 19:13 80:6 95:11 98:17 235:25 257:24 277:17 281:21 <b>conclusions</b> 209:24 234:10,25 278:14 <b>concrete</b> 8:5 133:20 143:9 <b>condition</b> 169:21 225:21 <b>Conditional</b> 226:7 <b>conditioned</b> 227:3 <b>conditions</b> 90:23 92:19 106:6,7 109:3 209:25 210:2 <b>conduct</b> 197:13 275:4 <b>conducted</b> 45:5 83:10,11 188:16 193:18 195:23 233:5 283:21 <b>conducts</b> 10:25 <b>conference</b> 3:18 4:13,15 5:19 6:21 13:15 63:16 94:22	108:15 112:24 128:6,14 299:7 <b>confidence</b> 93:24 146:20 147:23 <b>confident</b> 6:11 94:2 211:23 <b>confidentiality</b> 101:24 <b>confidentially</b> 34:5 <b>configure</b> 284:7,15 284:16 285:8 287:8,9 289:7,11 293:22 294:10,23 295:1,12 296:11 315:1 <b>configured</b> 253:12 <b>configuring</b> 288:16 <b>confirms</b> 229:6 <b>conflict</b> 32:2,11 183:4 <b>conflicts</b> 295:21 <b>confront</b> 51:5 135:14 <b>confused</b> 37:23 <b>Congress</b> 64:14 <b>connect</b> 114:22 <b>connected</b> 6:1 <b>connection</b> 10:4 <b>connections</b> 294:1 <b>Connectivity</b> 74:3 <b>cons</b> 198:19 <b>conscious</b> 171:1 <b>consciously</b> 111:6 <b>consensus</b> 56:18 63:9 <b>consent</b> 9:14 105:4 108:23,24 214:6 214:12 216:12,13 217:11 219:13 221:8 234:23 241:22 <b>consequence</b> 160:17 <b>consequences</b> 160:21 211:11,25 212:4,10 219:1 239:9 <b>conservative</b> 17:11	<b>consider</b> 50:25 85:17 107:12 154:13 297:21 <b>consideration</b> 184:21 193:2 <b>considerations</b> 134:4 <b>considered</b> 143:19 204:10 205:12 266:25 <b>consistent</b> 19:17 25:21 47:21 115:6 116:7 298:13 <b>consistently</b> 46:22 <b>consists</b> 153:4 174:19 <b>constantly</b> 6:8 <b>Constitution</b> 1:9 <b>constraint</b> 102:21 <b>constraints</b> 94:25 <b>construct</b> 206:7 207:17 217:13 <b>consulting</b> 43:19 <b>consumable</b> 166:18 <b>consumer</b> 6:20 7:20 8:3 11:8,20,22,23 20:17 32:13,18 33:17,20 34:3 37:24 40:15 43:4,4 52:20 56:2,14 63:14 66:3 68:7 89:9,13 96:16 98:1 98:11,18,24 100:1 102:8,9 104:18 108:10,11 109:13 109:19 116:5,24 118:9,12 120:21 121:1,2,9,11 122:7 122:8,9,25 123:2 124:21 131:3 174:19,22 203:11 203:17,20,22 204:1,1 206:12 207:9 208:15 210:25 225:22 230:11 233:8,19 234:14 239:17	241:23 <b>consumer's</b> 92:7 97:20 111:15 124:9 204:20 205:1 <b>consumer-depend...</b> 124:10 <b>consumer/company</b> 103:4 <b>consumers</b> 5:12 6:2 6:10,11,18 8:6,18 8:23,24 9:17,18 10:16 12:10,12,23 32:12,14 33:13 35:1,3,18,19 37:25 39:24 40:2,2 41:20 42:10 43:5 52:18 54:12,25 55:13 56:24 57:3,9 58:6 61:13,14,15,16 62:6,9 89:16,20 94:23 97:9 98:6 99:6,21 103:17,20 103:21 104:11 106:25 107:5,15 108:20 109:17 110:1,8,25 111:22 112:7,8 113:8,19 114:13 115:2,4,5 115:20 116:15 120:15 122:15 123:22,25 124:1 130:6 131:7,12,20 132:16,18,22 133:2,7,8,10 136:7 136:7 171:10 200:20 201:1,5 202:22,24 203:1,7 203:10 204:6,14 205:4,6,7,14,17,20 205:22,24 206:3,4 206:6,12,23,23 207:12,23 208:6,9 208:14 209:17,25 219:3,8 234:13 235:15 244:20,24 245:2,14,24 249:1	249:4,6 297:14 301:13,16 314:20 314:24 <b>consumers'</b> 2:11 8:14 43:2 55:3 56:8 68:2,8 112:2 112:6 113:3 115:18,25 116:17 122:18 132:20 133:18 201:11 203:13 204:8 241:7 <b>contact</b> 73:18 84:3 84:10 86:10,24 87:1 280:13,17 <b>contacted</b> 256:18 <b>Contacts</b> 253:17 <b>contain</b> 18:7 85:10 278:12 <b>contained</b> 236:10 318:6 <b>contains</b> 134:17 <b>contaminated</b> 114:14 <b>content</b> 52:23 171:11 233:12 265:21 311:23 <b>contents</b> 153:1 <b>contests</b> 10:9 167:2 167:3 <b>context</b> 72:3 81:14 89:10,14 100:23 100:24 106:9 107:3,8 108:21 109:22 164:25 239:18,20 241:8 271:4 275:7 286:2 294:8,14,16 <b>context-dependent</b> 12:3 210:4 <b>context-specific</b> 164:20 <b>contexts</b> 58:2 77:1 164:16 168:3 276:19,25 297:8 <b>contextual</b> 72:16 73:21 99:1 111:7
---	---	--	---	---

115:10 142:14 168:8 <b>contingent</b> 12:2 <b>continually</b> 116:7 <b>continue</b> 6:7 19:21 70:15 113:1 130:12 173:13 304:24 <b>continued</b> 13:5 <b>continues</b> 128:6 <b>continuing</b> 10:21 98:17,21 108:25 151:9 317:3 <b>continuous</b> 40:11 <b>continuum</b> 125:2 <b>contract</b> 90:21,22 102:10 105:23 111:14 120:14 121:18,21,24 228:15 <b>contracts</b> 105:17,25 106:4,16,20,25 107:6 108:4,6,11 110:5,7 111:12 114:2 121:13,20 <b>contractual</b> 64:21 <b>contradiction</b> 158:4 <b>contradictory</b> 276:18 <b>contrary</b> 112:7 <b>contrast</b> 48:21 103:15 115:17 190:12,18 192:12 192:18 194:20 196:6 <b>contrasting</b> 196:3 207:7 249:6 <b>contribute</b> 295:5 <b>contributing</b> 191:24 <b>contribution</b> 139:24 146:22 189:8 197:15 <b>contributions</b> 191:23 194:16 198:22 <b>control</b> 23:18 24:1 32:4 34:3 39:17	48:10,12 52:19 62:6,10 66:5 77:20 90:9 92:10,11 93:21,22,25 96:1 104:3,4,10,14,16 104:23,24 105:7 105:16,16 111:4 132:20,22 139:10 139:19 152:19 181:22 216:25 219:14,17,19 221:2,10 241:23 265:11 <b>controlled</b> 175:2,3 <b>controlling</b> 56:17 216:2,3,4,5 <b>controls</b> 217:22 231:8 245:16 247:7 297:8 <b>controversial</b> 34:16 <b>conundrum</b> 243:6 <b>convenience</b> 51:18 60:25 94:18 96:6 98:8 <b>convenient</b> 117:13 157:7 <b>convening</b> 305:3 <b>conventional</b> 250:19 <b>converged</b> 115:22 <b>conversation</b> 56:18 96:20 128:5,6 219:7 223:12 261:23 297:21,22 <b>conversations</b> 142:22 231:16 310:17 <b>converted</b> 255:7,8 256:6 <b>convince</b> 283:14 <b>convincing</b> 296:19 <b>cookie</b> 19:18 31:24 61:19 67:10 <b>cookies</b> 15:23 16:1,4 16:19,20 17:9,15 17:16,18,19,20,24 18:2,11,12,14,14 18:16,17,19,23	19:7,19 21:10 25:22 31:23,24 32:8 52:9,14 53:11 53:15 54:13 61:21 202:7 <b>cool</b> 54:10 252:22 <b>Cooper</b> 171:6 174:8 177:6 180:9 182:19 183:9,11 299:2 <b>core</b> 55:23 102:3 134:24 165:6 <b>Cornell</b> 159:23 260:20,20 <b>corollary</b> 147:12 <b>corporate</b> 42:18 126:17 224:2 <b>corporation</b> 117:24 222:5 <b>correct</b> 36:19 56:21 122:12 123:19 125:13 138:7,10 161:12,14 180:6 183:12,13 277:20 <b>correction</b> 186:11 <b>corrective</b> 143:1 186:17 <b>correctly</b> 37:7,7 167:17 <b>correctness</b> 156:10 156:10,12 <b>correlate</b> 18:4 <b>correlated</b> 144:15 162:5,8 <b>correlating</b> 152:14 <b>correlation</b> 78:6 144:16 152:18 160:13 218:18 <b>correlations</b> 173:14 173:17 285:9 296:1 <b>correspondence</b> 46:20 <b>corresponding</b> 221:10 <b>correspondingly</b> 219:14	<b>corresponds</b> 205:11 267:16 <b>cost</b> 12:22 50:1 227:20 229:24 230:6,6,7,10,14,18 231:5,9,13,18 232:5,9 233:1,20 234:25 235:2 282:4 306:25 <b>cost-benefit</b> 47:17 47:23 49:18 51:8 <b>costless</b> 307:2 <b>costs</b> 50:8 209:16,17 222:5 229:25 230:3,13,16,22 299:24 307:12 <b>couch</b> 229:24 232:16 <b>counseling</b> 218:23 <b>counselor</b> 218:24 220:18 <b>counselors</b> 300:8 <b>count</b> 18:12 <b>countermeasures</b> 9:23 <b>counterpoint</b> 309:3 <b>countries</b> 121:13 242:1 <b>countries'</b> 214:10 <b>country</b> 134:20 <b>country's</b> 101:18 102:4,9 <b>couple</b> 24:6 25:20 57:8 69:15 166:22 170:11 189:19,22 222:15 247:23 300:19 <b>coupled</b> 233:20 <b>coupons</b> 47:5 <b>course</b> 17:4 23:12 28:1 29:18 32:23 33:21 36:3 62:6 74:16 94:6 96:22 133:5 177:7 191:4 193:3,8 194:7,8 225:24 226:3 227:12 235:12	244:16 <b>court</b> 228:9,9,11 <b>courts</b> 228:3 <b>cover</b> 183:22 <b>coverage</b> 21:23 22:3 22:19 <b>covered</b> 235:9 291:20,20 <b>covering</b> 5:9 19:17 <b>covers</b> 36:11,12,12 <b>craft</b> 13:5 <b>Cranor</b> 2:6 13:1 44:8 313:24 314:2 314:8 <b>Cranor's</b> 52:25 <b>crashes</b> 25:22 <b>crawl</b> 16:24,24,25 17:1 28:18 <b>crawler</b> 17:7 <b>crawls</b> 25:16 26:10 28:25 <b>create</b> 15:20 45:18 46:14 56:15,21 138:18 153:9 155:6,11,12 162:2 176:6 182:17 215:14 264:9 270:12 <b>created</b> 10:22 126:19 148:11,14 211:12 212:18 213:17 311:13 <b>creates</b> 56:13 139:7 304:20 307:6 <b>creating</b> 108:3 161:8 174:21 179:17 223:19,24 307:13 <b>creation</b> 10:10 <b>creative</b> 238:10 247:20 <b>credit</b> 27:10 128:13 149:14 <b>crime</b> 32:9 <b>criminal</b> 226:11 228:8 <b>criteria</b> 302:24
---	---	---	--	--

<b>critical</b> 9:19 209:9 222:16 239:16	199:22 249:7 251:9,23 252:9 253:19,20 259:17 260:11 272:1 279:20 281:14 282:12 303:17	5:13,21 6:5,14 7:2 7:5,15,21,24 8:15 8:17,22,25 11:14 11:23 12:18,19,20 12:21 13:17 16:18 17:4 19:15 30:3,9 30:11 31:2 34:4 35:13 36:6 41:8,9 41:14,21,24 42:4 42:11,23 43:4,14 44:5,13 45:6 47:3 47:19,25 48:5,23 49:6,8,16 50:6,9 50:15 60:20,20 61:14 62:9 63:9,11 64:2 66:1,2,6,21 69:6,9,14 70:2,7 70:25 71:2,5,6 72:3,7,8,15,23,25 73:2,7,11,15,16,18 73:21,22 74:2,6,10 74:19,23,25 75:5,9 75:15,17 76:8,9,12 76:16,20 77:4,7,9 77:10,23,25 78:4,9 78:10,17,22,23 79:2,5,18 80:21,22 80:23 81:1,7,10,22 83:9,19,25 84:3,7 84:22 85:11,22 86:14,17,21,23 87:5,19,20,21,23 87:25 88:11,21 91:12 92:21,22 93:22 97:1,2,4,18 97:22,23 98:1,21 100:15,15,15,17 100:18,19,25 101:2,6,7,11,25 103:9 106:23 107:11,11,11,15 108:1 109:15,16 110:1 111:2 112:9 112:12 113:7 118:15,23 119:1,7 120:25 123:5 124:21,24 125:2	126:7,12,18,23 127:9,10,19 130:6 131:17 132:16,18 132:19,19 133:3,7 133:15,19,21,24 134:5 136:2,6,8,10 142:19 149:12 150:8,9,10 151:2,6 151:19 159:15 160:4 161:25 163:11 164:4 165:11,13,18,20 165:24 166:1,2,3,4 166:4,9 167:3,6 169:6,11,12 170:15,16,17 171:9,19,21,25 172:13,21 173:12 174:19 175:15 176:10,11,14,17 176:22 177:3,18 180:18 182:12 189:9 190:11 191:14,17 195:9 197:17 199:23,24 200:7,10,11,11 202:7 208:16 209:13,15,15,20 210:1,22 211:11 211:16 212:1,4,7,8 212:17,25 213:15 214:6,14,25 215:6 215:14 216:13,19 216:25 217:8 219:13,17 221:9 221:13 223:21,23 223:24 224:2,4,6,7 224:7,17 225:2,3 225:10,12,17 226:1,8,9,13,22 228:22 229:4,12 229:13,19,24 230:4,14,18,23 231:4,20 232:14 233:10 234:24 235:11,19 237:3,4 237:9,15 238:8	239:4,22 240:6,7 240:16,16,21,25 241:11 243:19 246:5,7 248:1,18 253:14 254:17,24 272:16,18 273:13 273:13 274:4,11 274:24 275:9 276:20 278:10,12 279:4,20,23,25 280:1,4,21 282:12 289:1 298:2 299:13 311:20
<b>cross</b> 117:12,22	<b>Curtis</b> 210:9	166:4,9 167:3,6 169:6,11,12 170:15,16,17 171:9,19,21,25 172:13,21 173:12 174:19 175:15 176:10,11,14,17 176:22 177:3,18 180:18 182:12 189:9 190:11 191:14,17 195:9 197:17 199:23,24 200:7,10,11,11 202:7 208:16 209:13,15,15,20 210:1,22 211:11 211:16 212:1,4,7,8 212:17,25 213:15 214:6,14,25 215:6 215:14 216:13,19 216:25 217:8 219:13,17 221:9 221:13 223:21,23 223:24 224:2,4,6,7 224:7,17 225:2,3 225:10,12,17 226:1,8,9,13,22 228:22 229:4,12 229:13,19,24 230:4,14,18,23 231:4,20 232:14 233:10 234:24 235:11,19 237:3,4 237:9,15 238:8	<b>data-driven</b> 65:13 65:24 149:24 150:23 159:18 160:9,20 161:8 162:1 163:4,10,10 165:8 166:23 167:21 170:25	
<b>cross-device</b> 8:9,10 53:24	<b>customer</b> 180:1,2	<b>data-generating</b> 225:10	<b>data-sharing</b> 276:23	
<b>cross-disciplinary</b> 131:6	<b>customers</b> 160:14	<b>data-wise</b> 44:1	<b>database</b> 102:25 228:7	
<b>cross-section</b> 235:16	<b>customers'</b> 42:21	<b>databases</b> 66:7 101:5,6 107:21	<b>date</b> 113:6 118:18 174:25 318:4	
<b>crosswalk</b> 117:20	<b>cut</b> 117:17 312:4	<b>DATED</b> 318:12	<b>Datta</b> 136:16,23 141:24 176:8 183:25 185:14 186:9	
<b>crowdsource</b> 176:21	<b>cuts</b> 296:9	<b>datum</b> 151:21	<b>Davi</b> 297:25 298:4 301:20 309:19	
<b>crowdsourcing</b> 84:20 176:18 274:5 277:23 281:23 297:13	<b>cutting-edge</b> 5:8 6:25 7:23	<b>day</b> 5:8 44:22 68:8 96:23 123:19 131:2 179:3 194:21 222:7 223:15 240:14 250:3 280:1 282:21 285:17 293:21,24 297:1 298:10 299:12		
<b>crowdworker</b> 278:25	<b>cyber</b> 12:22 222:6 222:11,17 223:13 223:14,24 224:5,7 224:13 225:20 232:25 233:1 234:25 235:2 316:1			
<b>crowdworkers</b> 275:15 276:2,8,10 277:4,6,7,10,19 278:3 279:3,10,15 280:19	<b>cycle</b> 125:21 133:17 197:8			
<b>crucial</b> 146:4 147:16 261:19	<b>cynical</b> 211:10 245:17			
<b>crucially</b> 204:4 305:15	<b>D</b>			
<b>cue</b> 97:23 98:3	<b>D</b> 2:1 3:1 318:17			
<b>cues</b> 95:3,12 96:7,13 96:19,24 97:10,12 98:19 99:2 124:19 125:3	<b>D.C</b> 39:4			
<b>Culture</b> 214:19	<b>dad</b> 53:9,10			
<b>cure</b> 209:20	<b>daily</b> 80:19			
<b>curious</b> 122:12,16 241:9	<b>Dan</b> 4:17,19 5:16 13:19 130:18 135:23,24 159:20			
<b>current</b> 2:9 7:2 11:19 14:2,10 78:7 81:3 84:4 86:10 114:24 250:12 251:4 259:20	<b>dancing</b> 99:16			
<b>currently</b> 74:4 76:25 78:12 123:14 138:21	<b>dangerous</b> 150:18			
	<b>dangers</b> 71:18			
	<b>Daniel</b> 159:16 182:15			
	<b>Daniel's</b> 173:24 180:14 185:18			
	<b>dare</b> 214:20			
	<b>dark</b> 51:3 150:22 277:15			
	<b>Darren</b> 110:17 125:18			
	<b>data</b> 2:13 4:23 5:9			

300:20 301:23 304:12 309:21,24 309:25 314:8,13 <b>days</b> 22:2 190:7 192:22 260:23 264:21 290:18,19 <b>DB</b> 93:7 <b>DC</b> 1:11 <b>de</b> 223:18 <b>de-</b> 63:10 <b>de-identified</b> 60:19 <b>de-identify</b> 60:6 101:2 <b>deal</b> 6:15 34:3 43:5 46:3 49:9 60:11 61:10 63:9,21 171:23 233:2 244:20,21 292:5 <b>dealing</b> 98:24 <b>deals</b> 47:20 <b>dealt</b> 63:25 <b>deaths</b> 99:13 <b>debate</b> 200:4 <b>debt</b> 232:19,21 <b>debug</b> 161:12 166:20 170:3,9 <b>debugging</b> 161:14 163:6 <b>decade</b> 134:20 <b>decades</b> 38:13 <b>decent</b> 208:1 <b>deception</b> 51:16 89:23 301:2 311:17 <b>deceptive</b> 5:13 9:3 9:10 <b>decide</b> 80:4 86:2 97:16 111:23 116:9 149:16 207:9 238:22 303:5 <b>decided</b> 144:18 186:5 216:9 261:12 <b>decides</b> 169:9 <b>decision</b> 72:19 199:18 204:2	215:7,21 216:23 218:7,10 300:15 302:24 307:21 <b>decision-making</b> 55:4 65:13,24 239:12 <b>decisionmaking</b> 33:20 37:24 <b>decisions</b> 7:11 23:21 32:15 33:5 36:8 54:17 62:11 89:2 110:9 131:7,17 132:3 144:24 172:7 182:4,13 199:11,20 215:1 239:3 299:20 302:23 303:8 304:22 <b>decisive</b> 213:12 <b>declare</b> 293:4 <b>decline</b> 47:20 <b>declining</b> 195:5 <b>decreases</b> 234:23 <b>decreasing</b> 196:6 209:21 226:17 229:5 <b>deemed</b> 101:20 108:13,23,25 <b>deems</b> 108:11 <b>deep</b> 16:24 17:1 133:13 <b>deepen</b> 11:11 113:9 <b>deeper</b> 89:15 177:20 184:19,19,20 274:17 <b>deeply</b> 142:4 172:2 <b>default</b> 34:11,13,18 55:8 <b>defaults</b> 287:17,17 <b>defense</b> 64:17 <b>defenses</b> 64:22 <b>defer</b> 65:15 <b>define</b> 82:22 96:16 115:16 164:15,16 164:19 182:2 222:11 <b>defined</b> 292:12	<b>defining</b> 224:14 <b>definitely</b> 23:5 61:7 66:17 96:8 113:18 113:24 161:4 197:16 246:20 <b>definitions</b> 33:8 <b>degeneration</b> 211:21 <b>degree</b> 11:22 140:11 149:21 242:22 307:23 <b>Deirdre</b> 143:7 171:7 171:13 174:8,13 174:17 <b>delay</b> 190:6 <b>delete</b> 60:7 <b>deleted</b> 32:8 <b>deleting</b> 53:15 <b>deletion</b> 31:25 80:23 81:3 84:2 86:14 87:3,4 <b>delighted</b> 5:17 <b>delineate</b> 97:22 <b>delirious</b> 57:12 <b>delivered</b> 218:21 <b>delve</b> 16:18 <b>demo</b> 159:10 <b>democracy</b> 59:6 <b>demographic</b> 91:12 93:10 127:19 144:21,22 <b>demographics</b> 91:19 93:10 <b>demonstrate</b> 42:9 272:24 <b>demonstrated</b> 115:12 <b>denial</b> 224:21 <b>denied</b> 8:24 77:16 77:18 <b>denigrated</b> 246:24 <b>denominator</b> 229:17 <b>department</b> 169:22 <b>departments</b> 134:23 169:24 171:18 <b>depend</b> 60:3 132:5 <b>dependent</b> 92:15	193:19 <b>depending</b> 124:25 155:18 221:15 287:2 <b>depends</b> 124:11 132:2 204:4 268:20 <b>depictions</b> 195:12 <b>deploy</b> 271:10 <b>deployed</b> 84:17 292:16 293:5 <b>deploying</b> 243:24 295:16 <b>Depot</b> 230:25 <b>depressed</b> 149:13 <b>depressingly</b> 211:19 <b>depression-related</b> 158:21 <b>derive</b> 204:16 <b>derived</b> 94:5,7 269:9 <b>deriving</b> 298:17 299:15 <b>describe</b> 33:10 57:8 140:2 174:12 280:16 286:19 <b>described</b> 279:4 309:20 <b>describes</b> 135:11 139:20 <b>describing</b> 84:6 299:25 311:12 <b>description</b> 167:7 182:15 <b>descriptions</b> 138:22 <b>descriptive</b> 235:19 310:21 <b>design</b> 80:1 99:5 125:14,14 135:11 146:15 172:13 235:17 281:18 309:1 <b>designed</b> 33:25 139:3 171:9 221:20 265:24 <b>designing</b> 154:17 161:25 172:18 175:14	<b>desirability</b> 300:17 301:5 <b>desire</b> 314:22 <b>desired</b> 83:8,14 84:12 88:19 <b>despite</b> 75:23 137:4 196:12,15 222:23 291:14 300:23 <b>destroying</b> 121:1 <b>detail</b> 16:18 40:15 40:19 43:18 197:18 198:24 270:6 271:19 286:20 <b>detailed</b> 131:6 <b>details</b> 3:7 132:15 152:12 156:24 190:8 276:13 279:8 <b>detect</b> 141:6 157:14 161:19 179:1 <b>detected</b> 17:15 152:24 225:21,25 239:22 <b>detecting</b> 160:11 162:24 <b>detection</b> 142:23 146:5 147:22 186:11,14 226:2 227:4 254:5 <b>detects</b> 151:19,21 <b>determine</b> 133:24 145:16 191:14 193:17 263:20 268:22 275:4 289:24 293:17 296:7 <b>determined</b> 202:17 203:25 263:17 <b>determining</b> 136:25 141:20 <b>determinism</b> 39:3 <b>deters</b> 221:10 <b>develop</b> 10:8 90:15 98:19 124:8,12 142:6 185:9 <b>developed</b> 16:23
--	--	---	--	--

24:7 59:15 133:19 147:1 222:17 279:13 285:2 290:7 316:3 <b>developer</b> 164:6,7 164:24 165:3,12 165:16 166:18 170:3 <b>developers</b> 161:11 162:21,22 163:4 170:9,20,23 185:24 197:10 271:9,17 313:8,13 <b>developing</b> 85:4 141:25 150:20 159:22 163:2 180:3 185:22 197:8 278:6 281:15 283:6 293:8 295:19 305:4,10 316:7 <b>development</b> 11:1 131:6 132:7 135:15 163:22 <b>developments</b> 10:6 11:4 <b>deviation</b> 287:13 <b>device</b> 7:25 71:20 133:7 250:23 251:20 252:17,22 252:25 254:2,23 254:25 255:8,15 255:18,21 256:6 256:10 257:1,5,5,9 257:14 259:4 260:10,12 265:2 265:13 266:8 267:6,9,22 268:2 268:14,22 269:13 269:16 308:9 311:23 <b>devices</b> 3:9 6:1 127:13 133:4,14 250:12,13,15,22 250:24 251:3,6,8 251:17 252:3,7,8 252:11,16 255:3	256:12 257:10 258:3,6,9,18,20,21 259:18,20 260:7,9 297:6 302:13,14 302:16 305:18 306:7,9,11 <b>devil's</b> 57:7 <b>diagnosis</b> 105:10 <b>dialogue</b> 7:4,6 72:17 <b>dialogues</b> 72:5,13 73:1 289:21 304:5 313:3,10,13 <b>diametrically</b> 90:17 <b>Dictionary</b> 48:17 <b>dictum</b> 46:17 <b>die</b> 99:12,17 <b>differ</b> 114:10 201:10 <b>difference</b> 91:17 101:14 104:21 115:14 139:18,21 140:20,25 146:17 146:18 177:19 179:2 190:3 261:19 263:7 311:21 <b>differences</b> 27:6,8 49:22 91:2 160:11 189:22 190:4,10 192:7 203:14 286:23 287:1 <b>different</b> 17:7 21:12 22:13,19 24:18 25:11,23 26:16 27:2,2,4,8 31:16 31:21 33:7 38:13 42:3 57:8 59:10 70:7 71:1 72:6 73:3 77:1 82:25 83:14,25 84:3,6 85:13 86:6 97:18 101:10 102:11 104:18 113:25 114:6,7 115:19 124:21 125:22 126:25 139:12 140:23 147:1 153:11 154:22	160:5,6 162:14 169:5 173:9,15,19 177:16,16 182:6 190:5 192:4 198:2 200:20 201:4,10 201:12,20 204:7 205:2,11,11 207:16 209:12,22 209:23 210:21,24 212:13 213:19 214:3,10,23 219:2 220:21 224:10,12 231:15 232:17 234:8,20 238:25 241:6,7,15,25,25 241:25 242:1,5 247:16 250:19 261:25 267:9 268:12 272:14,19 272:20,20 274:25 276:9,19,25 277:16 278:9 284:15 285:4 288:20 289:7 290:8,14 292:8,10 292:15,16 293:1 293:10 294:13,15 295:3,4,5,15 296:10 297:20 310:17 315:22,24 <b>differential</b> 176:25 184:13,14 <b>differentiate</b> 27:4 312:5 <b>differentiated</b> 152:16 <b>differentiator</b> 225:3 <b>differently</b> 85:16 89:18 121:24 201:13 287:6 316:21 <b>difficult</b> 42:25 59:20 81:4 138:23 165:15 172:6 240:19 251:2 258:2,7 273:8 277:1 287:8,9	<b>difficulty</b> 44:11 <b>diffusion</b> 220:23 <b>dig</b> 30:12,13 184:19 184:20 <b>digest</b> 307:25 <b>Digging</b> 177:20 <b>digital</b> 5:23 8:7 37:8 37:9 89:10,14 252:18 253:21 <b>dilemma</b> 60:24 240:14 <b>dimension</b> 104:16 <b>dimensions</b> 147:1 <b>direct</b> 109:13 175:15 216:7 257:19 301:1 <b>direct-to-consumer</b> 100:11 101:13,16 102:2,18 106:1 114:2 126:11 <b>direction</b> 96:9 239:11 246:20 313:16 <b>directly</b> 18:3 44:15 47:4 76:13 109:10 190:12 202:1 203:1 265:21 <b>director</b> 14:6 297:24 <b>disagree</b> 45:24,24 123:18 <b>disappear</b> 60:20 <b>disbanded</b> 121:14 <b>discern</b> 149:10 <b>disciplinary</b> 135:4 <b>discipline</b> 131:1 <b>disclose</b> 9:8 85:2 226:4 272:16 <b>disclosed</b> 226:2,6 248:6 <b>discloses</b> 81:1 <b>disclosing</b> 12:13 <b>disclosure</b> 190:6 224:18 226:7 227:2,3 245:19 297:9 305:13 306:1,25 <b>disclosures</b> 8:1	311:4,7 <b>disconnect</b> 30:4 95:19 311:9 <b>discontinue</b> 121:16 <b>discount</b> 45:11 46:24 47:2,8 <b>discounts</b> 46:8 48:1 48:21 50:14 <b>discover</b> 67:10 146:16,23 165:22 169:17 293:16 302:2 <b>discovered</b> 140:13 152:1 168:8 169:13,21 190:8 240:10 <b>discovering</b> 159:17 175:25 <b>discovery</b> 28:7 133:17 188:9,16 197:24 <b>discrete</b> 40:10 <b>discriminate</b> 216:20 <b>discriminating</b> 185:18 <b>discrimination</b> 50:5 66:22 107:16,25 145:6 147:3,11 171:12 173:5,21 173:21 183:19 <b>discriminatory</b> 8:19 142:13 143:10,18 <b>discuss</b> 15:21 100:13 136:13 218:24 301:8 <b>discussants</b> 171:6 <b>discussants'</b> 110:6 <b>discussed</b> 8:13 207:23 297:5 303:18 <b>discusses</b> 40:18 <b>discussion</b> 11:18 15:4 52:1 68:12 110:13 114:20 116:18 147:9 198:21,25 245:8 297:1
--	---	---	--	--

<b>discussions</b> 8:4 113:25 299:16 317:3	52:10 63:1 64:13 65:22 67:11,12,13 68:22 69:16 72:1 72:17,19 73:20 74:20 77:21 91:23 97:7 105:4 106:14 106:22 119:15,25 124:15 133:12 134:25 137:21 151:5 160:3,4 164:4 170:6 171:21 172:4 184:6 214:11 236:10 237:14,22 240:3 244:1 248:5 252:1 253:6 282:4 287:3 292:7 304:24 308:24 313:8,9,16	<b>draws</b> 27:1 <b>dream</b> 214:15 <b>drew</b> 57:2 <b>drink</b> 4:7 <b>drive</b> 58:4,4 131:24 220:6 280:6 <b>driven</b> 214:1 217:23 217:24 218:11,14 <b>driver</b> 57:14 <b>driving</b> 95:13 <b>dropdown</b> 293:9 <b>drug</b> 126:16 212:22 266:17 267:3,24 268:3,9 <b>drugs</b> 107:23 212:25 213:1 266:19 267:17 268:25 <b>DTC</b> 102:7,17 103:2 104:25 105:1,8,11 105:19 112:5 121:9 <b>dual</b> 11:8 <b>due</b> 56:24 75:12,19 77:8 201:1 <b>dumb</b> 99:12,17 <b>duplicate</b> 248:4 <b>duties</b> 101:23 <b>dynamic</b> 6:3 116:13 117:18 <b>dynamically</b> 263:17	220:22 236:14,18 247:11 283:8,20 286:11,13 288:8 290:9 <b>earned</b> 144:10 <b>earners</b> 144:7,14 <b>ease</b> 44:13 132:10 <b>easier</b> 24:17 28:4 29:14,21 135:3 278:3 294:15 303:5 <b>easily</b> 25:18 44:17 110:8 <b>easy</b> 109:2 135:2 161:17,18 276:21 288:20 <b>eat</b> 4:6 58:3 128:14 244:9 <b>eating</b> 40:22 <b>echo</b> 237:21 238:16 252:13 255:2 <b>echoed</b> 97:19 <b>econometric</b> 215:20 <b>economic</b> 12:21 200:10 201:3,8 210:11,21 221:18 234:12 236:20 238:24 301:4 303:7 <b>economics</b> 2:14 12:18 135:1 188:2 188:5 199:10 210:11 218:1 235:7,17,22 236:11 297:25 302:17 <b>economicus</b> 31:12 32:17 <b>economist</b> 210:21 215:24 217:3 298:21 <b>economist's</b> 214:15 <b>economists</b> 131:2 240:17 298:19 <b>ecosystem</b> 6:4 66:15 79:16 138:14,17 138:25 139:22	142:2,20 150:9 201:15 262:18 306:3 <b>ecosystems</b> 139:5,23 188:9 189:6,12 198:14 <b>edit</b> 138:8 <b>Edith</b> 5:11 <b>edits</b> 138:18 <b>educated</b> 122:8 <b>education</b> 49:21,23 95:23 105:9 119:16 190:23 227:25 228:4 <b>educational</b> 44:19 <b>effect</b> 40:14 119:3 147:5 166:11 168:15 169:23 216:22,23 217:22 219:16,19 220:3 221:14,18 238:4,5 240:22 245:3 264:11 <b>effective</b> 9:15 23:17 26:19,20 69:12 81:21 82:9,15 88:16 98:6 132:21 212:25 234:10 274:10 290:23 308:22,25 309:1 315:5,8 <b>effectively</b> 264:12 282:11 283:6 286:12,20 289:10 289:15 290:2,18 293:23 294:2,14 295:10,12,17 296:11,18 305:9 310:7,8 <b>effectiveness</b> 10:7 88:24 242:4 315:24 <b>effects</b> 40:13 111:8 133:25 140:2 142:2 146:16,24 165:22 175:25 210:21 218:14
<b>disempower</b> 183:8 <b>disorders</b> 267:1 <b>disparate</b> 141:6,9 173:6 184:14,20 218:17 <b>disparately</b> 134:1 <b>disparities</b> 9:1 181:5 181:6 <b>display</b> 106:25 130:14 139:12 281:17 <b>disprove</b> 208:24 <b>disregard</b> 237:13 <b>disrupt</b> 313:11 <b>disservice</b> 65:4 <b>distasteful</b> 34:17 <b>distinction</b> 82:3 83:3 153:25 <b>distribution</b> 5:3 230:22 <b>ditch</b> 153:1 <b>dive</b> 133:13 <b>diverge</b> 93:2 99:9 <b>diverse</b> 5:6 <b>diversity</b> 287:23 294:20 <b>division</b> 13:18 14:8 40:20 68:5 <b>DMVs</b> 228:2 <b>DNA</b> 100:21 103:5 106:12 107:9 108:3 120:23 <b>DNS</b> 257:6 258:10 <b>doctor/patient</b> 101:24 <b>doctors</b> 105:7,13 <b>document</b> 81:1 82:5 106:10 <b>doing</b> 15:8 20:8 21:20,21 22:6 23:14 26:10 28:22 28:24 29:8,25 30:25 40:8 41:17 44:5 45:14 47:3,24	<b>dollar</b> 230:8 <b>domain</b> 84:24,25 151:12 152:8 185:11 259:2 <b>domains</b> 82:24 <b>double</b> 18:19 213:10 289:17 <b>Doubleclick</b> 19:8 <b>doubly</b> 299:21 <b>Doug</b> 234:4 <b>download</b> 30:19 31:2 94:16 287:5 289:13 290:8 <b>downloaded</b> 283:17 <b>downloading</b> 108:7 252:24 253:8 <b>downside</b> 212:18 <b>DPIP</b> 13:18 <b>draft</b> 272:24 <b>dragged</b> 57:4 <b>dramatic</b> 15:22 258:1 299:24 <b>dramatically</b> 228:21 300:25 <b>draw</b> 27:15 33:9 114:4 220:10 238:24 <b>drawn</b> 148:7	<b>draws</b> 27:1 <b>dream</b> 214:15 <b>drew</b> 57:2 <b>drink</b> 4:7 <b>drive</b> 58:4,4 131:24 220:6 280:6 <b>driven</b> 214:1 217:23 217:24 218:11,14 <b>driver</b> 57:14 <b>driving</b> 95:13 <b>dropdown</b> 293:9 <b>drug</b> 126:16 212:22 266:17 267:3,24 268:3,9 <b>drugs</b> 107:23 212:25 213:1 266:19 267:17 268:25 <b>DTC</b> 102:7,17 103:2 104:25 105:1,8,11 105:19 112:5 121:9 <b>dual</b> 11:8 <b>due</b> 56:24 75:12,19 77:8 201:1 <b>dumb</b> 99:12,17 <b>duplicate</b> 248:4 <b>duties</b> 101:23 <b>dynamic</b> 6:3 116:13 117:18 <b>dynamically</b> 263:17	<b>E</b> <b>E</b> 2:1 3:1,1,23 120:4 120:7 318:1,1,1,17 318:17,17 <b>e-commerce</b> 106:20 <b>E1</b> 153:4 <b>E2</b> 153:4 <b>E3</b> 153:4 <b>eager</b> 5:23 <b>eagerly</b> 13:10 <b>eagerness</b> 316:10 <b>earlier</b> 83:23 220:24 299:3 <b>early</b> 15:18 52:2 59:25 102:18 103:18 215:16	

219:23 220:6,7 240:14,19,24 241:7,22,22 <b>efficacy</b> 93:21 96:1 <b>efficient</b> 80:1 192:3 223:9 244:6 294:23 <b>effort</b> 258:13 295:24 296:18 <b>efforts</b> 5:12 11:10 113:9 246:15 304:10 305:3,7 <b>Egelman</b> 68:16,21 118:13 122:21 126:24 <b>eight</b> 277:7 <b>either</b> 7:4 61:17 71:18 77:12 79:9 106:7 117:6 139:10 150:19 169:23 207:10,24 208:9 221:14 225:22 226:10 229:2 232:22 276:5 277:18 300:20 <b>Elana</b> 15:6 54:21 62:20 <b>electronic</b> 3:9 <b>electronics</b> 128:19 128:21 211:5 <b>element</b> 125:8 <b>elements</b> 74:5 285:24 286:11 293:10 294:16 295:5 <b>elicit</b> 84:21 <b>elicited</b> 83:18 <b>elites</b> 62:18 <b>email</b> 109:10 149:1 149:8 151:22 153:21,22,23 229:1 253:11,15 311:22 <b>emails</b> 148:6,7,12,14 148:21 152:15 153:1,2,4,7,11,12	154:3,12 155:2,4,8 155:10 157:14,16 <b>embarking</b> 11:5 <b>embraced</b> 220:24 <b>emerged</b> 91:23 <b>emergence</b> 188:23 <b>emergency</b> 3:17,20 <b>emerges</b> 173:10 <b>emerging</b> 6:9 8:5 186:12 188:21 195:12 <b>emphasize</b> 147:13 220:13 241:21 <b>emphasized</b> 284:3 <b>empirical</b> 19:15 115:1 188:8 189:11 200:15 208:22 209:4 213:22 220:14 222:11 223:5,13 236:25 237:2,2,18 238:1,14,21 314:17 316:11 <b>empirically</b> 35:14 116:8 125:8 <b>employed</b> 16:4 <b>employee</b> 180:20 <b>employees</b> 180:22 <b>employer</b> 216:20 <b>employment</b> 108:1 141:6 181:2,2,4,21 186:5 <b>empower</b> 170:22 172:12,17 174:2 <b>empowering</b> 307:4 312:11 <b>emulate</b> 175:1 <b>emulates</b> 214:10 <b>enable</b> 110:8 159:7 274:7 281:25 295:10 299:15 316:8 <b>enables</b> 157:11 173:8 <b>encounter</b> 108:5 119:24 123:3 <b>encountering</b> 294:8	<b>encourage</b> 13:8 97:4 115:7 191:5 198:5 219:20 250:16 258:23 304:25 313:12,19 <b>encouraged</b> 221:16 304:10 306:20 <b>encouragement</b> 135:5 179:21 <b>encouraging</b> 120:15 120:16 277:5 303:6 304:4 305:3 <b>encrypt</b> 132:8 <b>encrypted</b> 254:10 <b>encryption</b> 244:5 252:20 255:15,21 255:23 256:15 <b>end-users</b> 42:15 <b>ended</b> 22:5 30:5 73:15 250:12 254:25 <b>endless</b> 52:15 137:20 <b>endorsed</b> 97:24 <b>ends</b> 4:15 302:18 303:2 <b>enduring</b> 105:4 <b>energized</b> 195:18 <b>enforce</b> 117:4,5 251:1 255:21,22 258:3,16 259:7,9 260:6 273:2 <b>enforcement</b> 6:13 7:16 9:2,17 10:7 11:1 55:20 61:22 110:1 119:17 123:9 135:15 182:21 225:23 228:3 299:19 300:4,11,18 301:5 311:5 <b>enforcing</b> 255:19 <b>engage</b> 55:14 81:9 85:9 102:8 105:15 121:22 198:21 300:4 <b>engaged</b> 33:17	172:2 193:6 289:3 291:23 <b>engages</b> 85:8 102:7 <b>engaging</b> 55:5 107:13 225:7 303:17 <b>engineer</b> 247:6 <b>engineering</b> 135:1 261:16 262:21 312:4 <b>engineers</b> 298:20 <b>England</b> 58:5 <b>Englehardt</b> 20:2,4,5 61:1 65:17,25 <b>English</b> 81:1 <b>English-speaking</b> 45:4 <b>enhance</b> 278:2 <b>enhancing</b> 243:14 <b>enjoy</b> 6:11 <b>enjoyed</b> 115:7 <b>enlivens</b> 101:21 102:8,10 <b>enormous</b> 307:5 <b>enrichment</b> 228:15 <b>ensure</b> 6:10 8:17 11:12 13:5 55:17 56:1 80:4 185:18 258:7 <b>ensures</b> 205:22 <b>entail</b> 56:20 <b>enter</b> 254:9 286:1 292:14 293:15 <b>entered</b> 9:14 <b>entering</b> 242:20 <b>entice</b> 99:23 <b>enticing</b> 243:4 <b>entire</b> 134:23 168:9 179:12 184:7 217:13 287:18 291:2 297:11 <b>entirely</b> 192:15 293:1 312:22 <b>entities</b> 16:11,16 18:25 92:3,5 97:1 99:23 124:25 242:20,20 295:6	296:16 <b>entity</b> 143:16 248:8 263:12 293:1 <b>entry</b> 167:16,16 <b>environment</b> 51:2 58:4 94:24 131:14 219:2 250:19,20 295:9 <b>environmental</b> 308:5 <b>environments</b> 285:4 296:6,10 <b>envision</b> 30:22 <b>EPFL</b> 159:23 <b>equal</b> 91:15 155:13 181:2 195:6 199:25 <b>equally</b> 182:1,5,6 200:11 <b>equate</b> 105:16 173:14 <b>equates</b> 103:18 <b>equation</b> 78:19 93:11 123:12 <b>equations</b> 216:6 <b>equivalent</b> 140:2 295:12 <b>ER</b> 168:12 <b>era</b> 51:12,12 <b>eroding</b> 121:21 <b>error</b> 168:5,6,16 248:9 <b>errors</b> 279:12 <b>especially</b> 3:12 8:23 94:24 96:18 112:12 179:5 185:8 238:17 264:24 294:8 314:21 <b>essentially</b> 21:9 28:7 35:18 38:1 44:12 95:2 99:18 151:12 195:17 300:15 302:13,17,19 307:17 308:13 <b>establish</b> 310:7 <b>establishing</b> 214:6
--	--	---	--	--

214:15 <b>establishment</b> 184:15 <b>esthetics</b> 96:9 <b>estimate</b> 230:16 <b>estimates</b> 229:25 <b>et</b> 60:8 93:16 94:25 98:4 102:11 169:20 <b>ETags</b> 52:15,22 <b>ethical</b> 133:21 134:4 <b>ethnic</b> 47:15 <b>EU</b> 214:11 <b>Europe</b> 189:3 <b>European</b> 108:9 <b>evacuation</b> 3:20 <b>evaluate</b> 8:9 212:15 247:6 <b>evaluated</b> 155:22 <b>evaluation</b> 234:9,18 272:12 308:21 <b>evaluations</b> 226:19 <b>event</b> 3:11,16 4:11 4:17 5:1 13:20 31:16 224:13 225:20 226:4 232:7 314:6 316:19 <b>events</b> 222:11 223:24 224:2,5,7 224:12 225:25 226:9,23 227:13 227:20 231:17,22 232:25 233:1,21 235:1,2 <b>eventually</b> 71:13 242:24 289:1 <b>everybody</b> 5:18 99:1 130:10 <b>everyday</b> 42:2 48:3 51:2,5 <b>everyone's</b> 236:7 <b>evidence</b> 33:14,15 41:11 42:5 113:21 115:1 144:22 147:2 179:7 185:15 200:15	238:2 275:19 <b>evident</b> 174:10 <b>evolving</b> 116:10 <b>exact</b> 95:23 180:7 <b>exacted</b> 209:21 <b>exactly</b> 64:15 117:1 130:15 134:6 138:11 149:8 185:21 196:8 231:11 232:8,8 237:10 238:7 269:11 271:3 316:20 <b>examination</b> 184:7 <b>examine</b> 33:15 90:1 99:1 <b>examining</b> 134:14 184:3 222:5 <b>example</b> 9:24 17:5,7 23:7 37:5 42:8,20 47:1 76:2 81:10,14 81:17 82:19 84:5 86:13,17 87:8,9,12 87:18,24 88:7 89:22 92:8,13 107:23 132:7 135:6 137:10,23 140:12 146:16 148:4,20 149:12 149:15 150:5 152:20,25 153:16 153:17 154:10 155:2 158:13,15 158:24 159:9 160:19 166:21 175:18 180:12,19 181:10,12 182:11 183:2 184:2 189:9 197:7,21,25 211:18 213:4,4 224:21 240:7 241:20 245:15 252:25 253:9 254:19 255:3,12 255:24 256:8,20 258:14,23 259:25 268:25 283:20	288:8 309:5 <b>examples</b> 86:15 148:10 158:10,11 185:6 211:15,16 269:19 307:8 <b>excel</b> 200:9 <b>excelled</b> 131:19 <b>exception</b> 106:18 264:21 <b>exceptions</b> 226:5 <b>excess</b> 63:10,21 <b>exchange</b> 12:11 42:22 43:13 45:11 45:14 46:8 47:19 49:16 52:23 135:17 202:2,6,13 202:14 203:19 243:4 <b>excited</b> 58:15 95:14 95:15 132:24 141:24 <b>excitement</b> 58:17 <b>exciting</b> 36:13 <b>exclusionary</b> 8:19 <b>excuse</b> 35:11 <b>executive</b> 222:14 297:24 <b>exemplify</b> 154:25 <b>exercise</b> 40:23 103:3 132:22 302:22 <b>exercising</b> 131:13 <b>exhilarated</b> 57:11 <b>exist</b> 67:8 96:19 208:12 223:7 267:14 <b>existed</b> 268:2 <b>existence</b> 63:16 185:14 298:23 <b>existing</b> 8:25 36:20 101:22 126:8 219:10 235:18 305:24 311:3 <b>exists</b> 59:10 152:3 266:7,9 267:21 268:5,6,22,23 269:4 305:23 <b>exit</b> 3:22 77:14	<b>expand</b> 6:9 <b>expect</b> 14:14 21:24 48:21 74:24 81:9 81:10,18 82:1,2 83:6,7 86:13,21,24 87:4,9,22 117:4,9 117:20 119:23 120:2,4 123:2,12 127:23 132:16,17 136:8 179:13 285:21 314:21 <b>expectation</b> 78:16 82:22 83:5,12,13 97:20 114:9 115:16 117:2 118:2 124:9 206:18 275:6 <b>expectations</b> 2:12 11:20,22 63:14 68:2,9 78:2 79:6 80:2,13,17 81:8,13 81:16,23 82:12,14 82:22,23,25 83:2,4 83:10,18,23 84:12 84:21 86:8 88:19 88:20,25 90:7 98:18 100:1 111:1 111:24 112:3,4 113:25 115:2,6,12 115:14,18,21,25 116:5,16,17,25 118:14 119:13,25 122:24 124:21 126:1 127:4 142:14 275:5 285:11 293:17 294:5 297:17 <b>expected</b> 72:22 74:7 74:23 77:25 78:4 86:12 112:7 119:2 120:7 194:2 <b>expecting</b> 80:16 <b>expedite</b> 128:24 <b>expensive</b> 246:25 <b>experience</b> 94:9 276:6 286:7 <b>experiences</b> 53:19	53:20 94:10 96:4 124:11 264:25 302:1 <b>experiment</b> 140:10 140:14 148:10,18 <b>experimental</b> 139:11,19,25 146:15 177:2 <b>experimentally</b> 155:22 <b>experimentation</b> 212:13 213:19 <b>experimenting</b> 213:23 214:3 <b>experiments</b> 136:19 139:4 140:1 152:8 152:16 175:2,3 176:21 238:12 278:16 <b>expertise</b> 6:19 10:20 65:16 121:3 <b>experts</b> 5:20 8:12 10:12 11:18 55:1 84:24 132:14 276:5,12,15 <b>explain</b> 141:21,22 145:18 153:5 154:13 155:4,7,19 169:19 170:4 201:19 219:16 222:12 241:15 <b>explained</b> 8:12 <b>explaining</b> 31:23 220:11 <b>explains</b> 35:8 44:13 219:7 <b>explanation</b> 145:17 217:4,5,10 218:3 <b>explanations</b> 44:4 145:17 186:15 218:5 220:17 <b>explanatory</b> 36:7 94:10 170:7,14 235:20 <b>explicitly</b> 79:17 120:6 <b>exploding</b> 173:6
--	--	---	---	--

<b>exploitation</b> 301:4	231:24	<b>failed</b> 37:5	<b>faring</b> 57:9	<b>fell</b> 96:7
<b>exploited</b> 300:25	<b>extreme</b> 204:15	<b>failing</b> 111:11	<b>farm</b> 120:3	<b>fellow</b> 197:23 272:1
<b>exploits</b> 9:12 309:5	213:15	<b>fails</b> 38:18 63:13	<b>farther</b> 288:19	<b>felt</b> 92:2,5 286:13
<b>exploration</b> 89:20	<b>extremely</b> 140:7	<b>failure</b> 9:7 44:13	<b>fascinating</b> 14:15	<b>female</b> 140:16,21
280:1	157:7 283:24	<b>failures</b> 242:14	266:10	143:14 144:3,16
<b>explore</b> 89:24 191:7	289:22 306:3	245:2	<b>fashion</b> 188:22	144:19,21,22
<b>explored</b> 96:25	<b>eye</b> 125:11	<b>fair</b> 33:16 45:11,13	192:3 240:2	145:1,9
<b>exploring</b> 231:11		46:3 121:14	<b>fast</b> 120:19 127:3	<b>fewer</b> 37:6 80:4
<b>expose</b> 134:21	<b>F</b>	170:25 223:8	<b>faster</b> 94:20 128:21	94:10 155:18
295:10	<b>F</b> 318:1,1,17,17,17	302:3,10 308:6	267:4,7 278:3,15	196:14,15
<b>exposed</b> 74:5 179:21	<b>fabulous</b> 130:21	<b>fairly</b> 41:5 209:12	279:11	<b>field</b> 36:4 38:18
<b>express</b> 13:14	<b>face</b> 6:18 59:1 224:2	262:20 263:23	<b>faulty</b> 123:18	185:8 235:21
<b>expressed</b> 275:10	239:15	265:8,24 288:4,4	<b>favor</b> 117:19 180:5	236:1,12,19
<b>extend</b> 292:5	<b>Facebook</b> 19:8	<b>fairness</b> 134:4	212:21	240:14
<b>extended</b> 283:9	20:14 48:5 56:4	171:24	<b>faxing</b> 229:1	<b>fields</b> 134:18
<b>extending</b> 235:23	57:19 90:18	<b>FairTest</b> 159:19	<b>FCC</b> 51:17	<b>Fifty-two</b> 46:10
<b>extends</b> 235:18	118:22,24 119:2,7	163:3,21 164:3,19	<b>fear</b> 59:12 61:3 66:1	<b>fig</b> 50:21
<b>extension</b> 20:21	149:16 247:13	165:1,5,8,24 168:1	66:2	<b>figure</b> 20:20 37:10
25:3	252:23 295:8,18	169:6,16 170:2,6	<b>feasible</b> 277:24	42:25 44:1,19
<b>extensions</b> 25:25	296:4	170:11,19 172:11	<b>feast</b> 130:11	53:21 137:6
208:20	<b>faces</b> 240:15	176:4	<b>feature</b> 11:15 50:18	173:16 185:24
<b>extensively</b> 67:4	<b>facets</b> 11:7	<b>Faith</b> 313:23	170:14	230:8 269:14
<b>extent</b> 63:12 118:16	<b>facial</b> 7:24 54:3 56:6	<b>fake</b> 175:4,4	<b>features</b> 25:7,25	287:7
178:4 182:19	<b>facilitate</b> 112:25	<b>fall</b> 60:23 234:19	30:21	<b>figures</b> 230:17 232:3
200:25 209:10,11	201:17	<b>Fallacy</b> 41:3	<b>featuring</b> 11:18	<b>figuring</b> 80:7 314:25
241:16 305:25	<b>facilitates</b> 202:2	<b>falling</b> 26:2	<b>February/March</b>	<b>file</b> 266:4,7,9 267:14
315:11	203:2	<b>false</b> 39:24,25 56:18	45:3	267:16,21 268:1,5
<b>exterior</b> 185:23,25	<b>facility</b> 217:19	60:23	<b>federal</b> 1:2,8 5:19	268:6,6,22,23
<b>external</b> 188:17,19	<b>fact</b> 55:5,14 57:12	<b>familial</b> 100:21	15:19 31:14 39:20	269:4,4,15
197:10 264:22	63:15 64:22 66:25	<b>familiar</b> 21:7 25:4	39:20,23 97:6	<b>filed</b> 228:8,9
265:3,5,8,9,13,18	75:24 76:7 99:8	28:6 33:7 95:7	108:14 151:4	<b>files</b> 26:13 265:4,13
267:6,15 268:19	118:18 137:12	156:5 283:23	188:4 228:8,11	265:14,18 268:19
297:10	141:4 144:7	<b>families</b> 100:22	234:4 318:9	268:24 269:3,8,9
<b>extra</b> 29:19 153:9	155:16 179:25	<b>family</b> 90:13 100:24	<b>feed</b> 252:23	269:13 270:3
155:17	186:6 192:14	105:6 107:24	<b>feedback</b> 7:9 15:8	<b>filled</b> 6:25
<b>extract</b> 82:13 84:22	194:15 208:22	212:9	79:25 316:19	<b>fillings</b> 114:6,7
85:7 157:18	210:5 212:7,8	<b>famously</b> 33:21	<b>feel</b> 23:2 51:8 57:6	<b>filtered</b> 62:18
263:21,25 274:4	219:8 226:13	<b>Fandango</b> 9:5	92:24 96:10 128:4	<b>final</b> 100:6 159:15
276:22 277:1	231:24 233:19	<b>fantastic</b> 31:18	211:23 233:9	186:2 208:17
278:10,13 282:15	251:8 254:10	38:22	274:16 285:9	248:20 296:25
<b>extracted</b> 83:19	257:9 266:24	<b>FAQs</b> 158:6	286:5,22 287:6,15	<b>finally</b> 4:16 34:5,25
270:10	268:23 271:12	<b>far</b> 82:8 123:16	288:5 289:23	38:21 40:5,17 41:1
<b>extracting</b> 81:21	296:14	180:10 208:3	291:25 294:13	56:11 99:8 134:8
82:11	<b>facto</b> 223:18	212:3 224:6 227:1	296:1 301:21	203:7 207:14
<b>extraction</b> 278:2	<b>factor</b> 36:7	237:25 240:25	306:16	209:25 234:24
280:9	<b>factors</b> 194:7 197:10	246:11 261:10	<b>feeling</b> 55:16 57:9	235:15 297:15
<b>extraordinary</b>	<b>faculty</b> 183:22,24	265:22 270:21	<b>feels</b> 287:20	<b>finance</b> 227:22

<b>financial</b> 81:11 84:4 86:9 127:17 158:9 190:24 211:15 230:9,11 231:25	<b>finger</b> 257:13 <b>fingerprinting</b> 21:7 21:8,15 22:4,9,14 23:4 24:13 26:13 29:25 30:8 52:14 61:8,9,20,25	117:22 123:17 131:16 133:22 136:5 137:3 146:24 152:14,24 153:8 154:1 166:24 171:13 178:18 188:7,10 188:18 189:22 190:15,25 192:20 193:9,25 195:9 198:10 211:6,7 226:21 234:3 240:3 241:5 247:9 250:5 251:2 252:17 255:7 261:13 270:21,22 271:7 279:2 294:19 298:12 302:11 312:4 314:4	<b>flip</b> 78:13 97:9 <b>flocking</b> 57:22 <b>Florian</b> 271:25 284:2 285:15 297:11 309:20 <b>Florida</b> 89:8 <b>flow</b> 97:4 150:25 243:19 313:4 <b>flows</b> 137:6 138:20 140:3 257:7 306:2 <b>flu</b> 218:14 <b>fluke</b> 146:20 <b>focus</b> 21:7 64:1 66:21 67:4 81:8 119:13 142:20 143:4 186:13 188:25 189:16 194:14 201:15 215:7 235:14 274:10 278:18,20 280:22 281:19 282:8,9 <b>focused</b> 23:11 66:18 66:23 82:10 83:1 83:12 175:19 189:2 195:24 297:2,2 <b>focuses</b> 34:8 82:8 202:20 305:25 <b>focusing</b> 173:4 175:23 197:25 <b>folks</b> 54:6,9 66:17 126:14 236:24 <b>follow</b> 3:19 32:14 125:18 178:8 258:7 306:8 <b>follow-up</b> 127:11 242:8 279:7 <b>followed</b> 11:17 69:21 227:24 228:4 <b>following</b> 16:11 22:10 65:9 110:6 142:22 167:13,20 208:23 249:9 <b>follows</b> 202:4 <b>food</b> 4:7 114:13,14	114:19,19 128:15 <b>foods</b> 47:11 <b>forced</b> 103:3 132:13 <b>forcing</b> 302:25 <b>Fordham</b> 272:8 <b>foreground</b> 78:22 <b>forensics</b> 230:7 <b>forget</b> 302:9 <b>Forgets</b> 20:3 21:5 <b>form</b> 67:7 81:4 111:12,24 119:17 126:21 146:10 184:13 202:11 203:24 211:14 <b>format</b> 82:8,15 95:23 282:16 318:21 <b>formats</b> 82:10 <b>formed</b> 119:14 <b>former</b> 10:24 <b>forms</b> 50:6 60:19 139:2 210:24 213:16 219:12 311:16 <b>forth</b> 116:3 174:11 <b>forthcoming</b> 210:10 <b>forum</b> 299:18 <b>forward</b> 5:7 77:12 79:12 90:3 99:25 114:20 116:18 128:7 312:17 315:7 316:9 317:3 <b>found</b> 12:12 17:12 17:17 19:2,16 29:6 35:2 36:18 37:4 38:6 44:8 46:1,16 48:18 49:8,19,25 50:10,13 67:9 71:15 75:9,11,16 75:23 77:15 78:2,7 78:14 86:6,16 93:1 102:22 111:17,19 111:22 112:3,4,8 119:5 126:7 127:13 140:19 141:2,15 143:10 147:2 158:3,3,10
<b>find</b> 34:16 37:15,17 38:13 41:20 71:22 72:21 88:8 89:23 90:25 137:5,10 141:11 142:2 161:14 162:23 166:5,7 168:1 179:1,6 180:23 194:12 208:9 209:14,20 210:8 213:2 216:11 217:15 218:13 219:5,9 221:18,19 225:16 226:16 231:2,20 233:11 240:20,24 241:16 248:24 251:25 253:24 257:22 259:10,20 260:24 261:7 262:16 264:3 266:20 277:4,9,11 278:13 278:20 280:15 283:25 299:19 308:25 314:24	<b>firm</b> 43:20 111:8 179:25 225:5,7,20 225:21,22,24 226:4 230:4 233:20 245:3 <b>firm's</b> 204:17,17 233:2 <b>firm-based</b> 230:2 <b>firms</b> 43:2 200:20 208:4 222:25 223:1,6,15,17 224:1 227:5,16 230:25 231:6,16 231:21 232:12 233:9,17,21 235:14 243:22 244:11,15,15,15 244:22,25 245:13 245:23 246:4,5,14 301:15,16 <b>firms'</b> 242:9 245:9 <b>first</b> 3:8 10:14 14:5 14:10 15:8,24 22:23 23:24 24:7 27:19 29:20 31:22 34:8 43:23 45:7 47:8 54:7,21 59:23 64:17,17,21 65:7 66:25 68:16 72:14 72:25 76:25 78:8 78:10,20,21,22 83:4 90:2 93:9 100:12 101:14 110:23 111:10 113:14 115:13	<b>first-of-its-kind</b> 5:19 <b>first-party</b> 20:11 29:8 230:2 <b>fit</b> 308:10 <b>Fitbit</b> 57:16 126:12 <b>fitness</b> 57:17 <b>five</b> 11:15 35:3 43:22 88:11 116:14 148:13 190:13 215:2 236:23 245:21 252:11 257:12 270:9 278:11,18 290:12 296:5 <b>fix</b> 59:19 258:23 271:11 <b>fixed</b> 256:19,25 258:20 271:15 284:20,22 286:6 294:21 <b>Flash</b> 16:20 17:24 18:1,11 31:23,23 32:7 67:10 <b>Flashlight</b> 283:23 <b>flavor</b> 13:2 <b>flawed</b> 52:24	<b>flip</b> 78:13 97:9 <b>flocking</b> 57:22 <b>Florian</b> 271:25 284:2 285:15 297:11 309:20 <b>Florida</b> 89:8 <b>flow</b> 97:4 150:25 243:19 313:4 <b>flows</b> 137:6 138:20 140:3 257:7 306:2 <b>flu</b> 218:14 <b>fluke</b> 146:20 <b>focus</b> 21:7 64:1 66:21 67:4 81:8 119:13 142:20 143:4 186:13 188:25 189:16 194:14 201:15 215:7 235:14 274:10 278:18,20 280:22 281:19 282:8,9 <b>focused</b> 23:11 66:18 66:23 82:10 83:1 83:12 175:19 189:2 195:24 297:2,2 <b>focuses</b> 34:8 82:8 202:20 305:25 <b>focusing</b> 173:4 175:23 197:25 <b>folks</b> 54:6,9 66:17 126:14 236:24 <b>follow</b> 3:19 32:14 125:18 178:8 258:7 306:8 <b>follow-up</b> 127:11 242:8 279:7 <b>followed</b> 11:17 69:21 227:24 228:4 <b>following</b> 16:11 22:10 65:9 110:6 142:22 167:13,20 208:23 249:9 <b>follows</b> 202:4 <b>food</b> 4:7 114:13,14	

158:25 161:2	<b>free</b> 97:4 200:8	318:7	147:24 148:24	125:24 126:11
165:1 168:2	260:25 274:16	<b>fully</b> 289:20	149:7 159:4	210:18,25 211:16
211:19 213:8	<b>Freedom</b> 38:25	<b>fun</b> 36:10,11	174:23 180:15	212:5,22,24 213:5
214:2 217:9,12,15	225:16	<b>function</b> 8:12	184:24 185:21	213:7 215:1,4,7,8
218:10 219:3	<b>freezes</b> 25:22	163:15 227:22	186:18	215:10,22 216:15
220:12 221:7,13	<b>frequently</b> 12:14	228:1 232:13,15	<b>gee</b> 41:16 44:17 48:4	216:24 217:17,19
228:16 235:2	50:9 72:8 77:10	<b>functionality</b> 161:14	49:4	218:9,10,13,22,23
242:1 252:18	<b>fresh</b> 139:7	286:12 287:2	<b>gender</b> 49:21,22	218:23 219:25
256:16,18,20	<b>friend</b> 53:8 137:23	<b>functioning</b> 179:16	138:7,10 140:15	220:18 221:3,5,11
258:14 291:4,4,8	<b>friendly</b> 132:10	<b>fundamental</b> 190:3	144:16,17 146:17	221:12 234:19,23
316:18	281:10	243:6	164:12 167:22	239:16 241:8
<b>Foundation</b> 110:16	<b>friends</b> 56:3 105:6	<b>fundamentalists</b>	169:14 181:5	<b>Genetics</b> 102:15
<b>founded</b> 7:17	161:1	33:8 36:19 37:19	<b>gender-based</b> 147:2	<b>genuinely</b> 124:5
188:18 189:1,3	<b>friendship</b> 90:15	<b>fundamentally</b> 60:4	<b>general</b> 66:24	<b>Geoff</b> 298:7 301:25
<b>founder</b> 297:25	<b>front</b> 9:2 290:16	<b>funded</b> 272:5	102:13,19 103:22	<b>Geoffrey</b> 297:23
<b>four</b> 10:9 11:16	<b>front-line</b> 7:19	<b>funny</b> 36:18	104:1,5 121:5	298:4
43:20 45:21 57:1	<b>fruitful</b> 115:22	<b>further</b> 3:24 31:4	158:19 208:11	<b>geolocation</b> 202:8
57:20 68:10 84:3	<b>FTC</b> 3:14 5:11 6:8	41:11 68:15 89:20	214:22 221:7	<b>George</b> 171:6
109:9 127:7	7:14,16 10:9 11:12	94:12 157:22	224:1 234:20	183:21 234:5
192:20 196:1	39:9,15 62:13	198:21,24 203:11	242:11 303:15	<b>getting</b> 12:5 43:25
204:10 205:2	64:13,25 65:6	247:24 278:2	<b>generalizable</b> 239:5	59:14 61:4 132:9
207:17 229:8	66:17,23 97:24	279:1 290:4 292:3	242:4	176:9 181:25
234:8 284:11	99:25 100:13	<b>Furthermore</b> 256:5	<b>generalization</b>	211:21 213:14
288:11,11,13	113:16,20 116:8	<b>future</b> 15:9 19:21	42:20	231:6 233:9,13
302:4 303:9	123:24 130:16	30:10 31:1 50:18	<b>generalize</b> 292:3	240:6 242:12,12
<b>four-item</b> 92:10	135:12 150:16	56:10 69:10,14	<b>generally</b> 43:2 87:5	242:18 243:11,12
<b>four-wheel</b> 58:4	178:15 179:5	70:3 72:4 73:2	124:13 137:18	244:12 289:18
<b>fourth</b> 25:4 302:20	222:9 243:16	80:5 83:13 84:11	142:2 208:9	290:25 309:8
303:3 314:8	245:5 283:22	88:18 107:19,21	224:13 233:15	316:19
<b>fraction</b> 260:24	287:19 292:23	217:1 219:18	240:17	<b>Ghostery</b> 20:21
269:23 285:18,20	299:18 300:3,7,16	257:10 259:18	<b>generate</b> 81:20	26:19 30:5
289:2	301:18 304:2,3,23		<b>generated</b> 82:17	<b>GitHub</b> 30:18 31:6
<b>frame</b> 154:5 199:19	305:25 306:7	<b>G</b>	207:19 209:13	<b>give</b> 13:1 15:6 25:10
199:23,24 200:18	310:2,3 313:24	<b>G</b> 3:1	<b>generating</b> 134:16	26:23 27:10 42:3,3
252:12,18,19	314:4 316:24	<b>gain</b> 42:14	<b>generation</b> 5:25	45:10 46:8 48:4
253:7,13,17,21,23	<b>FTC's</b> 3:4 4:20 10:7	<b>galvanize</b> 55:13	<b>generational</b> 37:9	49:6,8 56:18 57:17
275:22	10:20 11:8 32:13	<b>Gandy</b> 36:5	<b>generator</b> 38:23	68:25 77:19 80:8
<b>frames</b> 200:4,14	68:6 125:6 180:18	<b>gap</b> 6:23 120:13	<b>generic</b> 151:18	85:22 103:15
209:3 254:16	300:11 313:22	316:24	159:6 268:17	111:15 116:1
<b>framework</b> 25:5	<b>FTC.gov</b> 4:14	<b>gaps</b> 236:3	<b>genericity</b> 156:22	123:10 125:16
222:17	<b>FTP</b> 254:17,18,20	<b>Gartner</b> 43:19	<b>genes</b> 213:9	134:8 138:10
<b>frameworks</b> 133:20	<b>fulfill</b> 6:20 92:6	<b>gateway</b> 256:9	<b>genetic</b> 100:11,15,16	140:12 149:17
<b>France</b> 214:19,20	113:8	260:1,2,5,5,8,12	100:18 101:5,13	156:7 160:6
<b>frankly</b> 33:18 65:3	<b>full</b> 87:18 94:20 98:9	<b>gather</b> 106:11	101:15,16,17,19	166:21 216:24
113:22 306:20	181:22 183:24	<b>gathered</b> 4:24	102:2,16,18,24,24	221:2 226:12
<b>fraud</b> 232:19,21,25	190:6 204:15	298:21	103:9 107:17,21	243:4 244:14
<b>Fraudsters</b> 10:2	246:18 273:8	<b>Geambasu</b> 147:21	114:2 121:4,6	245:25 259:11

272:12,13 274:12	178:18,24 180:10	79:12 91:8,13	19:24 31:13 68:4	<b>graduate</b> 169:7,9
274:19 275:15	183:21 186:22	92:25 94:2,3 98:13	70:25 71:11 77:12	276:7
277:14 280:23	194:16 198:24	100:14 102:20	89:11 99:3 101:4	<b>Graeme</b> 105:10
299:3 303:12	204:21 211:5	103:10 104:22	114:20 150:11	<b>granted</b> 69:19 71:17
307:18,24 314:6	212:3 215:21	105:22 110:19	167:16 171:2	73:1
<b>given</b> 3:24 10:19	219:11 220:18	111:2,3,24 112:25	174:1 185:17	<b>graph</b> 20:19 205:5
52:19 57:5 75:1	222:19 225:14	113:13 117:17	191:2 197:9 199:7	206:7
77:16 79:14 113:2	227:20 237:20	118:3 127:1	210:3 221:14	<b>graphical</b> 195:11
123:1 124:9	245:6 247:1 253:2	128:22 135:23	237:5,24 242:23	273:18
203:17 219:12,14	253:20 254:13,14	136:9,12,13,18,22	244:12 257:4,15	<b>graphs</b> 195:13
226:2 227:16	260:1 263:22	136:23 138:14,25	258:12,16 261:10	<b>gratitude</b> 13:14
230:13 285:12	264:2 266:18	140:12 141:22,25	264:11 265:22	<b>great</b> 5:6 6:15 15:10
301:22 307:18	270:6 271:17	142:20 143:2	276:3,20 282:24	26:6 38:23 43:12
308:2	273:20 276:13	147:15,20 159:21	287:25 289:25	58:24 71:10 80:7
<b>Givens</b> 15:18	281:12 288:18	160:6 164:15	307:1 308:10	99:11 117:25,25
<b>gives</b> 120:24 124:2	292:2,2 306:21	167:6 168:21	309:23 310:9	130:23 152:5
186:2 227:14	310:14,25 313:16	170:4,4 171:21	311:18 313:9,16	185:7 214:9 215:6
288:19	<b>goal</b> 9:20 13:12 16:8	172:22 177:8	<b>Google</b> 19:2,4,7,10	222:9 223:4
<b>giving</b> 47:22,25 50:9	42:15 75:13 122:9	178:5,7,8,24 182:5	48:17,17 57:19	230:15,15 233:2,6
102:24 105:4	122:11,11 150:23	182:6,16 183:14	58:21 137:11,11	277:18 286:19
117:5 119:7	164:19 244:16	199:25 209:1	137:14,15,25	294:9 313:15
123:22 198:9	272:24 274:18	210:23 213:13,18	138:1,7,8,10,25	314:10
214:18 217:17	281:24 303:20	214:4,25 215:3,19	140:5,6,17 141:16	<b>greater</b> 16:15 18:20
221:8,9,25 276:1	<b>goals</b> 131:12 147:16	216:3,13 217:3,20	143:17 144:2,3,17	40:15,19 247:5
278:25 311:18	175:16,17 274:17	218:2,4,16,19	160:3,24 161:4	307:6
<b>glance</b> 198:10	<b>God</b> 244:12	219:14,20,23	165:17 182:24	<b>greatest</b> 16:16 18:25
<b>global</b> 232:19	<b>goes</b> 27:1 52:20	220:1,6,7,14,23	247:13 255:22	227:11,11,17,23
<b>Gmail</b> 148:5,11,15	61:21 66:9 114:5	223:10 229:23	256:13 263:11	228:3
149:10 152:5	123:8 128:7	235:23 240:22	266:16 271:15	<b>greatly</b> 39:22
157:10,12,15,16	169:23 186:10	241:4 252:10	295:7,18	<b>green</b> 205:16 207:11
157:17,20,24	239:11 259:10,14	254:12 257:2,5,12	<b>Google's</b> 18:21 19:2	<b>grim</b> 57:2
158:5	302:5 311:11	260:1 264:2 270:5	19:6 143:17 145:7	<b>grocery</b> 46:9
<b>go</b> 23:25 24:16,22	<b>going</b> 14:16,21,22	272:3,12 274:15	160:22,23	<b>gross</b> 23:2
26:14,24,25 27:24	15:11 17:12 20:1,6	275:11 276:13	<b>gorillas</b> 161:3	<b>Grossklags</b> 188:7,10
29:22 30:18 39:10	20:25 21:3 23:19	279:25 281:2,18	<b>governed</b> 71:7	239:7 242:17
41:5 43:18 46:7	24:5,15 26:10,15	282:13 283:13	105:17	246:12 247:8
52:5 54:3 66:4	26:23 28:3 29:11	284:23 285:11	<b>government</b> 38:4,15	<b>ground</b> 27:25 75:3
67:11 85:6,21	30:2 31:4,11 32:24	286:19 287:3,6,20	50:4 54:11 57:24	210:7 302:21
88:16 91:4 94:1,2	35:25 37:8,10	288:18 289:12	62:14 92:4 97:2	<b>ground-breaking</b>
94:15 99:24 103:3	38:13 41:2,4 44:2	292:9 293:24	101:24 190:23	135:8
103:5,8 105:13	48:6 51:25 53:14	294:9 297:12	216:19 227:24	<b>group</b> 13:16 19:18
123:6 124:12	53:20 54:6,21 57:7	298:11 300:8	228:1 234:6	37:12 38:25
138:8,9 139:16	59:12,13 60:6,7	307:3 310:25	245:11 259:9	139:11,19 143:24
142:24 144:12,13	61:4,23 64:18,19	311:6 312:17	<b>GP</b> 105:11	144:6,9,11 150:20
145:20 146:8	64:20 66:12 67:17	313:14 316:8	<b>GPs</b> 72:23 73:18	241:4 242:7
147:11 150:24	70:24 72:14 77:12	<b>gold</b> 238:6	76:1,4,13,18 121:8	277:19 288:4
156:23 176:9	77:13 78:11,24	<b>good</b> 3:3 5:17 14:3	<b>grad</b> 276:11 277:10	<b>group's</b> 106:3

<b>groups</b> 8:22 26:6 36:20 37:20,20 51:20 104:18 107:24,24 139:11 139:21 140:21 281:19 288:5,11 288:12,13 307:4	<b>habituated</b> 69:25 70:6 <b>habituation</b> 77:13 <b>hacker</b> 190:1 <b>HackerOne</b> 188:24 189:2,23,24 190:16 191:4,13 192:18 193:12 194:16 195:14 196:4,14,20	174:22 185:4 237:16 252:20 304:17 306:4 <b>happens</b> 12:14 27:22 70:17 86:20 101:12,15 132:19 133:6 150:8 151:2 206:14 266:17 269:7 270:16 293:19 309:25	101:20,25 106:2 107:11,14 109:22 126:6,7,19,22,22 158:9,16 166:25 167:4 211:15 212:2 213:17 215:13,14 216:20 227:24 235:11	193:16 221:21 223:15 282:8 285:23,24 286:4 294:11 302:23 303:19 305:25 313:12 315:19,23
<b>Grover</b> 250:6,8 306:5 <b>grow</b> 124:5 <b>growing</b> 52:7,7 101:1 <b>grown</b> 146:25 <b>guarantee</b> 61:24 156:9,9,10 <b>guaranteed</b> 40:23 296:14 <b>guarantees</b> 295:23 <b>guard</b> 128:22 <b>guess</b> 23:16 29:13 61:2,10 62:21 65:25 66:8 68:25 114:20 117:3 118:13 122:23 127:1 156:6 158:9 177:9,15 183:11 185:17 241:3 242:16 244:23,23 303:10 304:2	<b>hackers</b> 189:25 191:16 197:1,23 <b>hail</b> 57:13 60:14 <b>hair</b> 181:17 <b>half</b> 12:7 63:18 112:5 140:15,16 179:9,10 192:20 232:3,25 233:2 262:10 <b>hallway</b> 4:5,9 128:15 <b>hand</b> 11:3,4 58:16 105:22 151:1,1,3 172:10 198:14 219:11 221:20 275:16 282:8 292:25 304:24	<b>hard</b> 13:20 28:16 58:15 79:16 130:17 149:1,9,10 150:15 161:19 162:20,25 211:13 211:16 243:7 263:20 283:13 290:22 291:10 302:3 309:1 <b>hardening</b> 246:15 <b>harder</b> 191:13 <b>hardware</b> 76:13,19 250:25 251:13 306:15 <b>harm</b> 59:5,6 65:11 65:21 66:18 71:24 177:14 179:4,7 180:7,9 183:2 184:15,21 186:8 211:17 224:20	<b>health-related</b> 103:1 <b>hear</b> 12:24 13:2 20:1 31:11 41:2 54:5,16 54:18 58:12 68:10 80:12 89:6 132:24 135:20 142:6 147:20 302:11 <b>heard</b> 26:6 38:25 62:16 94:21 110:20 124:9 128:9 131:21 149:18 160:10 171:8 191:15 222:14 261:22 281:3 302:4 314:12,15,17,19 314:19 315:6,7,9 315:10,12 316:10 316:17	<b>helped</b> 9:3 134:9 147:4 <b>helpful</b> 28:5 122:16 197:16 280:5 <b>helping</b> 7:10 9:19 131:19 <b>helpless</b> 281:3 <b>helplessness</b> 55:16 56:9 118:17 119:9 <b>helps</b> 238:4 241:17 275:21 278:14,20 <b>Heritage</b> 167:4 <b>heterogeneity</b> 205:10 <b>heterogeneous</b> 205:6,7,20 311:19 311:20 <b>heterogenous</b> 206:24 <b>heuristic</b> 97:23 124:3,7 <b>heuristics</b> 122:16 123:16,18,22 124:1,19 <b>hey</b> 22:21 23:14 24:22 29:24 116:25 178:5 260:9
<b>guidance</b> 8:6 133:20 133:23 <b>guide</b> 10:25 51:14 131:16 200:22 <b>guided</b> 6:14 <b>guidelines</b> 97:17 98:2,19,20 99:25 124:20 125:7 <b>guy</b> 53:12 <b>guys</b> 26:7 62:24 66:10 115:3 122:12,17 124:6 125:16 148:19 159:11 242:9 259:1 267:19 311:13 314:9	<b>handful</b> 239:4 <b>handle</b> 192:12 <b>handled</b> 6:12 192:22 276:19 <b>handout</b> 258:14 <b>happen</b> 24:6 54:12 56:10 61:11 62:1 118:4 161:6 173:7 182:16 239:20 251:11 316:8 <b>happened</b> 22:3 101:17 126:16 137:7 162:7,8 169:12,13 269:25 <b>happening</b> 5:4 11:24 23:13 28:14 29:6,24 61:11 66:6 75:2 76:25 78:12 111:25 123:5 136:8,10 149:20	<b>harming</b> 166:12 <b>harmless</b> 265:8 <b>harms</b> 56:20 168:20 275:2 299:1 <b>harvest</b> 192:2 <b>hashing</b> 8:13 <b>hats</b> 188:17 298:1 <b>head-hunter</b> 178:12 178:13,23 181:13 <b>heading</b> 258:2 <b>heads</b> 49:4 189:9 <b>health</b> 57:17 58:3 64:18 81:12,12,18 84:4 85:2 86:9 87:10,13 101:18	<b>hearing</b> 134:10 316:17,22 318:8 <b>hears</b> 32:3 39:3 <b>hearts</b> 33:22 <b>Heather</b> 89:6 92:25 100:4 111:21 124:6 <b>heavily</b> 95:16 132:6 <b>held</b> 8:8 10:9 127:15 228:22 <b>Hello</b> 15:14 20:4 41:4 80:15 147:24 272:2 <b>help</b> 6:20 8:4,17 9:22 10:12 11:4 24:3 30:1 31:5 54:17 81:6 99:11 113:19 134:17 162:23 166:20 170:2 185:24	<b>Hi</b> 250:9 260:21 <b>hiding</b> 10:5 250:22 <b>hierarchical</b> 93:8 95:22 <b>high</b> 96:6 131:15 140:10 144:7,14 152:11,13 167:18 191:19 205:9,10 205:10 229:11 233:20 248:10 280:15 <b>high-paying</b> 146:18 179:21
<b>H</b>				

<b>high-quality</b> 248:18	250:18 251:6,8,10	<b>hosted</b> 7:22	<b>I've</b> 107:6	<b>ignored</b> 291:17
<b>high-severity</b>	251:11,21,22	<b>hosting</b> 222:9	<b>IAPP</b> 15:5	<b>ignoring</b> 291:19
191:12,24	252:1,8 257:23	<b>hosts</b> 18:15,18	<b>Ibrahim</b> 15:12,15	<b>illegal</b> 9:24 141:9
<b>higher</b> 95:23,23	259:25 260:14	<b>hotel</b> 149:4	<b>icon</b> 76:5,7,13 95:9	<b>illustrate</b> 152:21
96:4 143:13	297:7	<b>hotspots</b> 76:17	96:12 125:7,9,14	169:5 170:2
144:25 169:15,25	<b>homes</b> 252:9 254:4	<b>hour</b> 77:8	<b>icons</b> 44:20 98:5,7	<b>illustrated</b> 63:22
194:21 219:24	<b>homo</b> 31:12 32:17	<b>hours</b> 75:7 192:20	99:22 125:3	<b>image</b> 160:22
231:9,17,18,23	<b>homogeneity</b> 205:10	<b>house</b> 257:20 260:2	<b>ID</b> 183:22	163:13,20 267:16
232:9	<b>homogenous</b> 206:5	<b>housekeeping</b> 3:7	<b>idea</b> 32:14,20 38:2	<b>images</b> 160:24 265:1
<b>highest</b> 180:2	206:13	<b>houses</b> 255:5	41:7 43:24 45:9,23	<b>imaginable</b> 310:13
202:15 206:11,22	<b>homosexual</b> 149:6	<b>housing</b> 173:21	46:22 47:25 52:20	<b>imagine</b> 22:21
234:22	158:14	<b>Hsu</b> 159:16,20	54:23 55:3,9 56:11	178:21 212:24
<b>highlight</b> 7:13 8:20	<b>homosexuality-rel...</b>	<b>HTC</b> 9:4	60:11 62:17	214:21 230:5
88:24 112:11	149:8	<b>HTML5</b> 16:19	115:11 122:10	232:20 267:8
119:1 142:17	<b>homosexuals</b> 158:14	17:23,24 18:3,4,11	152:13 183:5	294:9 295:20,24
143:8 145:18	<b>honestly</b> 14:19	27:2 31:25 52:14	276:3 281:16	<b>immediately</b> 20:16
147:3,4 180:12	<b>honored</b> 144:3	67:10	282:5 285:1,5	195:11,19 270:14
194:1 278:11	<b>Hoofnagle</b> 31:11,13	<b>HTTP</b> 16:19 17:14	293:14 301:25	300:22
280:24 285:23	59:21 63:24 65:15	18:14,19 253:2	<b>ideal</b> 265:15 293:20	<b>impact</b> 6:10 63:13
<b>highlighted</b> 33:12	67:3	254:15 255:17	312:15	85:16 86:8,12
277:19	<b>hook</b> 44:16	<b>HTTPS</b> 255:16	<b>ideally</b> 293:7	109:14,17 127:17
<b>highlighting</b> 81:21	<b>hope</b> 5:5 7:4,5 30:24	256:15	<b>ideas</b> 135:17 146:15	135:6 141:7,9
82:11 112:15,17	31:1 113:1 128:5	<b>hub</b> 7:19 252:12	<b>identifiability</b> 212:7	168:25 169:23
173:3 278:6	135:15 164:5	257:2,3,16,23	<b>identifiable</b> 101:1	173:6 177:21
285:24	185:7 226:7 243:9	<b>huge</b> 43:6 149:25	<b>identification</b> 63:10	178:21 179:1,12
<b>highlights</b> 219:15	271:18,21 281:19	150:9 155:14	<b>identified</b> 236:12	179:17 184:14,21
316:16	292:18	186:15 211:8	271:12 311:9	185:11 193:8,17
<b>highly</b> 131:20	<b>hopeful</b> 94:13	212:19 213:16	<b>identifier</b> 100:20	199:14 200:18
143:19 147:16	<b>hopefully</b> 98:4	275:11	<b>identifies</b> 10:25	231:16 248:13
181:14	113:4 282:3	<b>hugely</b> 215:13	<b>identify</b> 9:3 21:12	315:14,20,25
<b>historical</b> 169:4	293:24	<b>human</b> 29:20 133:1	68:12 82:13,23	<b>impacted</b> 86:8,13
<b>history</b> 39:19 74:7	<b>hopes</b> 96:6 111:2	<b>hundred</b> 268:7	83:20 100:21	<b>impacts</b> 315:22
121:15 173:20	<b>hoping</b> 112:24	<b>hundreds</b> 52:11	135:9 212:25	<b>imparts</b> 137:14
176:23,24	274:23 280:8	79:22 238:24,25	229:14 234:11	<b>impetus</b> 89:14
<b>hit</b> 53:7 99:11,18	<b>horizontal</b> 203:12	<b>HVAC</b> 292:25 293:2	274:24 276:21	<b>implement</b> 69:3,12
<b>HIV</b> 218:7	203:19 204:11	<b>hyper-competition</b>	299:1 310:1 311:6	79:13 132:14
<b>hold</b> 18:5 140:8	205:18,21 207:25	43:12	<b>identifying</b> 9:25	247:10 251:3
181:8 183:21	<b>horse</b> 119:12 212:14	<b>hyperlink</b> 122:1	146:5 298:22	258:10 260:4
202:8 277:5	214:23 241:13	<b>hyphenation</b> 318:20	312:3	273:23 303:20
<b>holders</b> 200:11	242:2	<b>hypotheses</b> 45:2	<b>identities</b> 10:5	<b>implications</b> 39:8
<b>holding</b> 300:15	<b>hospital</b> 167:9,12,20	<b>hypothesis</b> 48:2	<b>identity</b> 14:9 68:6	50:25 55:11 68:14
<b>holds</b> 140:9 203:6	167:23,25 168:12	156:15	107:22 270:15	110:22 240:16
203:21 298:1	217:19 232:19	<b>hypothetical</b> 145:14	<b>if/then</b> 94:14	241:10 257:25
<b>home</b> 16:1,25 17:2	<b>hospitals</b> 167:7	<b>hysterectomy</b>	<b>ignorant</b> 58:7,10	298:17 301:1,11
17:13,17 18:15	217:6,11,16	213:11	<b>ignore</b> 70:9 71:13	301:15
28:11 53:7 90:12	218:17 221:11		81:5 161:24	<b>imply</b> 56:22 265:16
135:16 230:25	<b>host</b> 18:23 101:22		273:10	<b>importance</b> 7:13
		<b>I</b>		

10:19 51:19 <b>important</b> 4:24 9:18 11:2 19:10 51:5 58:13 82:20 85:12 85:15 91:20,24 92:9 95:2 99:9 101:19 105:1,8 109:13 132:3 133:5,8 134:11 140:6 142:23 146:11 153:25 155:15 165:11 168:18 172:10 173:2 189:22 201:14 205:9 208:21 217:14 220:13 235:10 239:3 240:13 243:8 271:1 275:20 298:15 299:23 300:18 301:4 305:13,15 311:9 313:2 <b>importantly</b> 55:1 90:19 92:15 134:22 154:20 172:1 191:25 <b>impose</b> 245:3 305:5 <b>imposed</b> 230:12 <b>imposes</b> 312:5 <b>impossible</b> 101:3 <b>impractical</b> 77:6 <b>impressions</b> 144:18 145:12 158:1 <b>impressive</b> 13:16 <b>improper</b> 230:20 <b>improve</b> 20:8 110:5 222:16 242:13 245:13 250:17 259:18,20,23 310:15 <b>improved</b> 72:10 196:16 <b>improvements</b> 194:25 <b>improves</b> 45:18 <b>improving</b> 195:8	198:17 241:23 <b>IMS</b> 64:18 <b>in-depth</b> 189:11 197:14 <b>in-house</b> 39:22 <b>inability</b> 52:18 67:5 <b>inaccuracies</b> 8:21 122:19 <b>inaccurate</b> 122:15 122:20 <b>inadequate</b> 308:4 <b>inappropriately</b> 108:2 <b>inattention</b> 106:25 <b>inboxes</b> 157:12 <b>incapable</b> 251:13 <b>incentive</b> 233:22 244:22 312:12 <b>incentives</b> 12:21 133:16 196:13,15 223:6,6,7 231:6 235:14 243:2 244:16,17 245:13 249:5 273:22 301:12,15 304:21 315:25 <b>inch</b> 247:23 <b>incident</b> 161:2 223:23 227:15 228:1,3 <b>incidents</b> 12:22 222:6 224:19 225:4 226:18,21 226:23 227:3,22 227:24 229:5 <b>inclined</b> 248:17 <b>include</b> 64:21 109:5 109:6 110:3 111:1 224:5 229:25 230:1 262:3,11 308:21 <b>included</b> 8:11 20:12 225:11,11 <b>includes</b> 11:3 <b>including</b> 8:22 36:5 54:25 57:23 109:20 133:10	201:5 246:19 269:22 270:15 298:2 304:15 <b>income</b> 160:14 162:6,9 180:24 220:9 <b>incoming</b> 256:17,21 <b>incomplete</b> 227:14 <b>inconsistent</b> 46:19 <b>incorporate</b> 111:13 116:16 262:8 <b>incorporated</b> 7:15 <b>incorporating</b> 261:1 <b>incorrect</b> 50:10 75:12 122:6 123:10 <b>incorrectly</b> 50:4 85:25 <b>increase</b> 18:3,4 97:8 98:4 148:2 151:1,3 194:2 196:9 221:3 221:4 223:3 227:2 <b>increased</b> 18:13,22 18:24 62:17 <b>increasing</b> 43:3 52:18 62:25 99:23 101:4 107:20 200:6 201:2 206:19 226:13,17 226:24,24 228:21 <b>increasingly</b> 6:3,16 43:10 50:15,22 102:5 200:7 <b>incredibly</b> 13:16 130:17,17 133:8 142:18 <b>incumbent</b> 118:12 <b>incur</b> 230:4 <b>independent</b> 153:13 188:22 193:20 310:16 <b>India</b> 137:9,16 140:19 141:18 178:7 <b>indicate</b> 49:15 <b>indicated</b> 91:2 144:1 144:6	<b>indicates</b> 48:14 300:11 <b>indicating</b> 142:9 <b>indication</b> 76:20 93:7 <b>indicative</b> 196:16,23 <b>indicator</b> 124:5 <b>indicators</b> 75:24 76:1,2 112:14 <b>indirect</b> 240:17,19 <b>individual</b> 80:2 101:19 102:7 131:12 156:11,12 209:17 214:1 217:22 <b>individually</b> 100:20 208:4 <b>individuals</b> 44:15 54:24 89:18 103:9 131:16 132:4,8 216:25 220:24 <b>individuals'</b> 47:13 <b>industries</b> 125:22 227:9,10 232:17 233:3 <b>industry</b> 8:3 63:12 63:12 64:7 97:25 106:18,22 108:16 113:3 120:11,18 121:16 209:22 227:7,14,16,23 232:24 236:4 237:3,4,10,19 273:21 <b>industry-specific</b> 106:21 108:5 126:9,21 <b>ineffective</b> 315:6 <b>inevitable</b> 48:16 <b>infancy</b> 244:4 <b>infer</b> 56:15 76:15,18 79:22 157:19 191:18 240:8 268:23 270:2 <b>inference</b> 238:6 269:20 <b>inferences</b> 47:15	138:17 148:7 <b>inferred</b> 79:20 138:6 144:17 <b>inferring</b> 299:2 <b>influence</b> 54:17 218:9 <b>influences</b> 199:19 <b>inform</b> 8:4 29:23 81:25 82:1 260:8 274:18,19,20 282:11 308:17 311:8 317:2 <b>information</b> 5:2 6:12 10:1 12:4,6 12:11,13,15 17:6 18:5,6,7 22:16 32:13 33:16 35:21 38:5,5,24 39:18 40:9 42:9,13 44:14 45:12,17 46:9,14 47:23 50:10 54:1 57:17 59:15 60:4,5 60:7,15,16 61:4 62:11 65:23 68:24 70:10 71:14,18 72:17,18 74:5 76:4 81:11,12,19 84:3,4 84:10,14,16 85:3 85:18,20,25 86:1,9 86:10,19,25 87:1 87:10,14,18,19,21 88:3,5,10,13 90:8 90:9 92:7,12,23 94:21 105:9 110:16 112:6,13 119:22 123:23 126:13 136:25 137:6,17 138:6,9 138:11,21 139:20 139:22 140:3 141:19 149:14,16 150:1,3,25 158:8 167:11 171:17 173:10 181:6,20 188:13 199:12 200:2,5,10 201:1 201:11 202:10
--	---	---	---	--

203:12,13,14,19 203:21,23 204:4,8 204:11,12,13,14 205:18,22 206:3 206:11,15,17,22 206:25 207:9,11 207:12,13,18,25 208:3,5,6,10,11 215:12 218:20 221:2,8 224:19,24 225:13,16,17,24 230:1 231:25 233:14 234:15 236:21 237:7,11 245:19,25 246:1,6 246:23 247:2 249:10 250:15,18 251:7,10,14,19,20 251:22 252:4,5,16 253:9,25 254:1 256:1,14,23 257:11,20 260:1 260:13 261:3 263:4,21,25 265:2 266:7,12,13 270:2 270:5,10,14,18 271:6 273:14 274:11,12 278:12 279:23 280:13,17 280:23,25 281:2 282:15 283:18,25 284:13 285:10 286:14,16,23,24 292:17,20 293:2,5 293:12 296:3 297:9 305:14,20 305:21 306:1,2 307:5,6,19,24 308:2 309:3 310:23 313:3 316:13 <b>informational</b> 109:21 131:11 205:3,12 207:24 <b>informative</b> 5:8 203:10 <b>informed</b> 7:11 50:1	52:21 54:3,23 58:8 62:10 103:10 110:9 123:23 214:5,12 216:12 216:12 219:12 221:7 234:22 241:22 272:17 293:19 <b>informing</b> 272:23 <b>informs</b> 7:18 69:8 <b>infrastructure</b> 19:2 19:5 24:8 25:7 30:17 151:12 157:3 182:9,10,18 222:16 292:8 293:8 294:16,17 295:5 <b>infrastructures</b> 150:22,24 151:8 151:11 184:7 185:3,10 <b>ingest</b> 94:24 <b>inherent</b> 117:13 258:19 <b>inherently</b> 66:16 100:25 258:3 <b>initial</b> 36:5 195:14 196:21 198:23 <b>initially</b> 256:21 <b>initiated</b> 189:23 196:7 <b>inject</b> 182:20 <b>injury</b> 64:22 <b>innovation</b> 6:11 60:3 110:16 <b>innovative</b> 10:13 13:6 60:13 <b>input</b> 7:7 164:8 175:5 <b>inputs</b> 152:14,17,19 155:14,19,25 163:11,16,23 167:22 172:5 174:18 175:5,21 175:25 176:1 <b>insecure</b> 9:8 <b>inside</b> 146:2 195:2	251:6,21 252:1 256:3 257:23 260:2 262:6,14 264:6,8,10,13 <b>insight</b> 274:17 <b>insights</b> 6:19 58:14 113:2 134:17 <b>Instagram</b> 90:18 <b>install</b> 69:7,25 70:12 70:18 72:1 76:23 <b>installing</b> 53:15 70:15,19 <b>instance</b> 12:7 25:12 31:22 35:20 71:19 71:20 118:20 127:21 141:9 143:9,11 168:20 200:5 244:5 257:7 264:7 269:23 283:16 284:8 285:14 286:2 287:1 289:14 292:18 304:6,7,17 305:1 309:21 <b>instances</b> 25:14,14 139:8 142:12 172:24 184:10 245:12 <b>instill</b> 248:15 <b>Institute</b> 68:17 <b>institution</b> 143:1 <b>institutional</b> 44:12 102:25 <b>institutions</b> 62:18 92:3 95:25 134:9 135:16 190:23,24 190:24 <b>instruction</b> 3:24 <b>instructions</b> 3:19 <b>instructive</b> 197:13 <b>instrument</b> 233:6 <b>instrumentation</b> 25:18 <b>instrumented</b> 73:10 73:13 <b>insufficient</b> 162:16 <b>insurance</b> 108:1	168:22,23 212:2 216:21 223:13,14 223:23 227:7,23 232:1 <b>insureds</b> 227:8 <b>integral</b> 200:24 <b>integrate</b> 163:4 170:18 <b>integrated</b> 306:15 <b>integrating</b> 313:3 <b>integration</b> 197:9 243:25 302:15 308:6 <b>integrity</b> 115:10 142:14 <b>intellectual</b> 224:22 <b>intellectually</b> 154:9 <b>intelligent</b> 79:10 <b>intend</b> 183:12 <b>intended</b> 133:22 <b>intending</b> 161:4 173:7 <b>intensifies</b> 207:1 <b>intent</b> 183:7 <b>intention</b> 102:23 <b>intentional</b> 150:19 173:5 <b>intentionally</b> 143:17 291:18 <b>interact</b> 6:5 80:19 80:20 139:13 189:15 203:16 296:10 <b>interacted</b> 83:15 <b>interacting</b> 77:2 189:20 <b>interaction</b> 103:4 143:6 202:20 273:5 294:25 313:7,11 <b>interactions</b> 133:2 270:19 294:22 <b>interacts</b> 313:6 <b>interconnected</b> 274:14 <b>interdisciplinary</b> 11:2 134:24	<b>interest</b> 15:10 51:18 193:8 204:21 208:13 227:21 245:10 249:3 267:24 274:24 295:21 <b>interested</b> 56:11 97:7 146:3 181:25 200:14,25 202:8 210:6 223:16 225:1 236:6 252:15 282:6 310:3 316:17,19 316:22 <b>interesting</b> 18:12 46:11 54:22 60:19 64:1 103:3,15 104:16 108:14 137:6,10 141:14 158:20 160:15,15 168:17 176:19 179:24 181:12 192:7,23 198:3 204:23 211:4,7 215:10 232:2 239:19 240:15 255:14 257:8 261:9 266:3 276:14 296:1 298:9,15 302:11 308:12 309:2 310:25 313:17 314:17 <b>interestingly</b> 102:22 104:14 190:21 226:23 303:4 <b>interests</b> 150:4 207:4,7 305:9 <b>interface</b> 254:13 255:3,4 279:15 294:21 <b>interfaced</b> 255:15 <b>interfaces</b> 131:25 279:10 <b>interfering</b> 182:4 <b>intermediaries</b> 200:21 201:5
--	---	---	--	---

<b>intermediary</b> 201:15 202:1,21 203:2,4 204:7,18 207:8 208:1,13,15 248:25 249:3,4	<b>interviewing</b> 119:6 <b>interviews</b> 90:3 91:6 91:8,9,24 94:5,8 95:6 133:1	<b>involving</b> 141:14 <b>iOS</b> 72:12 75:25 <b>IoT</b> 127:13 250:18 251:17 253:18 257:10 259:1 283:10 284:24 286:2 292:3 294:8 294:16,20 295:3 297:6 302:13 305:2 306:7,11	291:25 294:13 297:5 <b>itdidn't</b> 95:4 <b>items</b> 4:2 94:5,19 98:8 <b>iterative</b> 281:18 <b>ITIF</b> 125:20 <b>iTunes</b> 101:9	<b>Joe</b> 36:12,12 41:2 51:24 52:1,17 62:19,25 63:8 <b>Joe's</b> 53:5 58:8 <b>Joel</b> 275:2 <b>joining</b> 171:5 <b>joint</b> 136:22 188:12 199:8 210:23 283:11
<b>intermediary's</b> 205:1 206:8,10,16 206:19,21	<b>introduce</b> 15:11 19:14 68:15 135:24 234:4 248:13	<b>IP</b> 9:25 28:7,10 202:7 <b>iPhone</b> 57:14 <b>IPP</b> 63:17 <b>irrespective</b> 190:6 <b>irrevocable</b> 101:7 <b>isolation</b> 271:2 <b>ISP</b> 253:5,20 257:22 259:14 260:3	<hr/> <b>J</b> <hr/> <b>jail</b> 236:9 <b>James</b> 171:6,13 174:6 177:4 299:2 <b>Jan</b> 40:16 100:7,10 109:18 110:12 112:4,16 <b>January</b> 1:6 280:2 318:4 <b>Japanese</b> 103:14 104:20 <b>jargon</b> 273:8 <b>Jasmine</b> 89:7 98:20 100:5 111:22 <b>Jasmine's</b> 111:11 <b>Java</b> 9:8,12,16 <b>JavaScript</b> 26:12,13 26:21 28:9,17 29:16 32:1,7 <b>jaywalkers</b> 117:11 <b>jaywalking</b> 117:12 117:14,22	<b>Jolie</b> 213:4,7 <b>journal</b> 62:22 210:11 240:23 <b>journalist</b> 157:13 <b>journalists</b> 26:8 51:14 144:8 <b>journals</b> 299:9 <b>JP</b> 230:25 <b>JPEG</b> 254:16 <b>juggle</b> 301:23 <b>Julie</b> 12:25 130:4 <b>jump</b> 63:5 198:20 287:19 <b>jury</b> 198:6 <b>just-in-time</b> 313:10 <b>justification</b> 299:19 <b>justifies</b> 43:4,17 <b>justify</b> 41:7 50:22 <b>Justin</b> 14:5 64:24 130:18
<b>intermediate</b> 270:24	<b>introduced</b> 201:17 <b>introduces</b> 146:14 <b>introducing</b> 145:6 <b>introduction</b> 68:21 <b>intuit</b> 47:4 <b>intuition</b> 155:23 205:19	<b>issue</b> 9:13 19:15 41:19 65:24 70:23 118:13,16 119:10 119:20,21 123:7 124:4 127:2 170:15 182:10 191:7 198:20 209:21 239:16,18 251:4 277:22 304:6 306:6,19	<b>January</b> 1:6 280:2 318:4 <b>Japanese</b> 103:14 104:20 <b>jargon</b> 273:8 <b>Jasmine</b> 89:7 98:20 100:5 111:22 <b>Jasmine's</b> 111:11 <b>Java</b> 9:8,12,16 <b>JavaScript</b> 26:12,13 26:21 28:9,17 29:16 32:1,7 <b>jaywalkers</b> 117:11 <b>jaywalking</b> 117:12 117:14,22 <b>Jens</b> 188:7 199:4 234:9 240:12 246:21 <b>Jens'</b> 243:12 <b>JO</b> 318:15 <b>job</b> 31:18 58:23 119:15 130:20,23 141:11 177:16 178:2,6,7 212:2 248:5 311:18 313:9 314:5,10 <b>job-related</b> 143:12 146:18 184:1 <b>jobs</b> 94:25 140:18 144:13 178:17,19 178:24	<hr/> <b>K</b> <hr/> <b>Kaifu</b> 199:8 <b>keen</b> 223:13 <b>keep</b> 14:22 25:21,22 27:5 151:6 152:25 196:18 266:1 314:2 <b>keeping</b> 195:6 <b>kept</b> 131:25 <b>Kevin</b> 188:4 235:5 <b>key</b> 8:4 9:24 16:9 19:22 22:15 33:1 51:1,11,15 102:21 112:17 131:3 274:4 304:4,11 305:8 314:16 <b>keys</b> 124:1
<b>internally</b> 6:16 143:22 247:6	<b>intuitive</b> 152:13 <b>invasive</b> 88:6,9 <b>invest</b> 310:19 <b>invested</b> 175:20 <b>investigate</b> 210:24 261:12 <b>investigated</b> 261:11 315:22 <b>investigating</b> 197:22 200:14 209:19 240:5 262:19 <b>investigation</b> 3:5 4:21 9:13 10:23 14:7 94:12	<b>issued</b> 7:22 8:15 133:21 <b>issues</b> 7:20,23 11:7 11:21 12:2,20 40:19 51:15,16,17 55:10 59:22 63:25 102:16 104:2 106:22 112:22 114:24 118:11 119:12 131:3 133:21 134:7 135:9 160:8 161:13 171:23 177:9 179:4 211:3 212:6 250:4 270:4 274:21,22 275:3 282:10 285:13 287:16 288:6	<b>Jan</b> 40:16 100:7,10 109:18 110:12 112:4,16 <b>January</b> 1:6 280:2 318:4 <b>Japanese</b> 103:14 104:20 <b>jargon</b> 273:8 <b>Jasmine</b> 89:7 98:20 100:5 111:22 <b>Jasmine's</b> 111:11 <b>Java</b> 9:8,12,16 <b>JavaScript</b> 26:12,13 26:21 28:9,17 29:16 32:1,7 <b>jaywalkers</b> 117:11 <b>jaywalking</b> 117:12 117:14,22 <b>Jens</b> 188:7 199:4 234:9 240:12 246:21 <b>Jens'</b> 243:12 <b>JO</b> 318:15 <b>job</b> 31:18 58:23 119:15 130:20,23 141:11 177:16 178:2,6,7 212:2 248:5 311:18 313:9 314:5,10 <b>job-related</b> 143:12 146:18 184:1 <b>jobs</b> 94:25 140:18 144:13 178:17,19 178:24	<hr/> <b>K</b> <hr/> <b>Kaifu</b> 199:8 <b>keen</b> 223:13 <b>keep</b> 14:22 25:21,22 27:5 151:6 152:25 196:18 266:1 314:2 <b>keeping</b> 195:6 <b>kept</b> 131:25 <b>Kevin</b> 188:4 235:5 <b>key</b> 8:4 9:24 16:9 19:22 22:15 33:1 51:1,11,15 102:21 112:17 131:3 274:4 304:4,11 305:8 314:16 <b>keys</b> 124:1
<b>internals</b> 137:5 145:22 147:13,14	<b>intuitive</b> 152:13 <b>invasive</b> 88:6,9 <b>invest</b> 310:19 <b>invested</b> 175:20 <b>investigate</b> 210:24 261:12 <b>investigated</b> 261:11 315:22 <b>investigating</b> 197:22 200:14 209:19 240:5 262:19 <b>investigation</b> 3:5 4:21 9:13 10:23 14:7 94:12	<b>issued</b> 7:22 8:15 133:21 <b>issues</b> 7:20,23 11:7 11:21 12:2,20 40:19 51:15,16,17 55:10 59:22 63:25 102:16 104:2 106:22 112:22 114:24 118:11 119:12 131:3 133:21 134:7 135:9 160:8 161:13 171:23 177:9 179:4 211:3 212:6 250:4 270:4 274:21,22 275:3 282:10 285:13 287:16 288:6	<b>January</b> 1:6 280:2 318:4 <b>Japanese</b> 103:14 104:20 <b>jargon</b> 273:8 <b>Jasmine</b> 89:7 98:20 100:5 111:22 <b>Jasmine's</b> 111:11 <b>Java</b> 9:8,12,16 <b>JavaScript</b> 26:12,13 26:21 28:9,17 29:16 32:1,7 <b>jaywalkers</b> 117:11 <b>jaywalking</b> 117:12 117:14,22 <b>Jens</b> 188:7 199:4 234:9 240:12 246:21 <b>Jens'</b> 243:12 <b>JO</b> 318:15 <b>job</b> 31:18 58:23 119:15 130:20,23 141:11 177:16 178:2,6,7 212:2 248:5 311:18 313:9 314:5,10 <b>job-related</b> 143:12 146:18 184:1 <b>jobs</b> 94:25 140:18 144:13 178:17,19 178:24	<hr/> <b>K</b> <hr/> <b>Kaifu</b> 199:8 <b>keen</b> 223:13 <b>keep</b> 14:22 25:21,22 27:5 151:6 152:25 196:18 266:1 314:2 <b>keeping</b> 195:6 <b>kept</b> 131:25 <b>Kevin</b> 188:4 235:5 <b>key</b> 8:4 9:24 16:9 19:22 22:15 33:1 51:1,11,15 102:21 112:17 131:3 274:4 304:4,11 305:8 314:16 <b>keys</b> 124:1
<b>international</b> 68:17 108:20 234:7 297:24	<b>intuitive</b> 152:13 <b>invasive</b> 88:6,9 <b>invest</b> 310:19 <b>invested</b> 175:20 <b>investigate</b> 210:24 261:12 <b>investigated</b> 261:11 315:22 <b>investigating</b> 197:22 200:14 209:19 240:5 262:19 <b>investigation</b> 3:5 4:21 9:13 10:23 14:7 94:12	<b>issued</b> 7:22 8:15 133:21 <b>issues</b> 7:20,23 11:7 11:21 12:2,20 40:19 51:15,16,17 55:10 59:22 63:25 102:16 104:2 106:22 112:22 114:24 118:11 119:12 131:3 133:21 134:7 135:9 160:8 161:13 171:23 177:9 179:4 211:3 212:6 250:4 270:4 274:21,22 275:3 282:10 285:13 287:16 288:6	<b>January</b> 1:6 280:2 318:4 <b>Japanese</b> 103:14 104:20 <b>jargon</b> 273:8 <b>Jasmine</b> 89:7 98:20 100:5 111:22 <b>Jasmine's</b> 111:11 <b>Java</b> 9:8,12,16 <b>JavaScript</b> 26:12,13 26:21 28:9,17 29:16 32:1,7 <b>jaywalkers</b> 117:11 <b>jaywalking</b> 117:12 117:14,22 <b>Jens</b> 188:7 199:4 234:9 240:12 246:21 <b>Jens'</b> 243:12 <b>JO</b> 318:15 <b>job</b> 31:18 58:23 119:15 130:20,23 141:11 177:16 178:2,6,7 212:2 248:5 311:18 313:9 314:5,10 <b>job-related</b> 143:12 146:18 184:1 <b>jobs</b> 94:25 140:18 144:13 178:17,19 178:24	<hr/> <b>K</b> <hr/> <b>Kaifu</b> 199:8 <b>keen</b> 223:13 <b>keep</b> 14:22 25:21,22 27:5 151:6 152:25 196:18 266:1 314:2 <b>keeping</b> 195:6 <b>kept</b> 131:25 <b>Kevin</b> 188:4 235:5 <b>key</b> 8:4 9:24 16:9 19:22 22:15 33:1 51:1,11,15 102:21 112:17 131:3 274:4 304:4,11 305:8 314:16 <b>keys</b> 124:1
<b>internationally</b> 108:18	<b>intuitive</b> 152:13 <b>invasive</b> 88:6,9 <b>invest</b> 310:19 <b>invested</b> 175:20 <b>investigate</b> 210:24 261:12 <b>investigated</b> 261:11 315:22 <b>investigating</b> 197:22 200:14 209:19 240:5 262:19 <b>investigation</b> 3:5 4:21 9:13 10:23 14:7 94:12	<b>issued</b> 7:22 8:15 133:21 <b>issues</b> 7:20,23 11:7 11:21 12:2,20 40:19 51:15,16,17 55:10 59:22 63:25 102:16 104:2 106:22 112:22 114:24 118:11 119:12 131:3 133:21 134:7 135:9 160:8 161:13 171:23 177:9 179:4 211:3 212:6 250:4 270:4 274:21,22 275:3 282:10 285:13 287:16 288:6	<b>January</b> 1:6 280:2 318:4 <b>Japanese</b> 103:14 104:20 <b>jargon</b> 273:8 <b>Jasmine</b> 89:7 98:20 100:5 111:22 <b>Jasmine's</b> 111:11 <b>Java</b> 9:8,12,16 <b>JavaScript</b> 26:12,13 26:21 28:9,17 29:16 32:1,7 <b>jaywalkers</b> 117:11 <b>jaywalking</b> 117:12 117:14,22 <b>Jens</b> 188:7 199:4 234:9 240:12 246:21 <b>Jens'</b> 243:12 <b>JO</b> 318:15 <b>job</b> 31:18 58:23 119:15 130:20,23 141:11 177:16 178:2,6,7 212:2 248:5 311:18 313:9 314:5,10 <b>job-related</b> 143:12 146:18 184:1 <b>jobs</b> 94:25 140:18 144:13 178:17,19 178:24	<hr/> <b>K</b> <hr/> <b>Kaifu</b> 199:8 <b>keen</b> 223:13 <b>keep</b> 14:22 25:21,22 27:5 151:6 152:25 196:18 266:1 314:2 <b>keeping</b> 195:6 <b>kept</b> 131:25 <b>Kevin</b> 188:4 235:5 <b>key</b> 8:4 9:24 16:9 19:22 22:15 33:1 51:1,11,15 102:21 112:17 131:3 274:4 304:4,11 305:8 314:16 <b>keys</b> 124:1
<b>Internet</b> 7:24 10:4 19:11 43:7 45:15 53:24 133:14 137:12 139:12,13 184:8 200:6 250:10 258:15 272:9 284:20,24 294:21	<b>intuitive</b> 152:13 <b>invasive</b> 88:6,9 <b>invest</b> 310:19 <b>invested</b> 175:20 <b>investigate</b> 210:24 261:12 <b>investigated</b> 261:11 315:22 <b>investigating</b> 197:22 200:14 209:19 240:5 262:19 <b>investigation</b> 3:5 4:21 9:13 10:23 14:7 94:12	<b>issued</b> 7:22 8:15 133:21 <b>issues</b> 7:20,23 11:7 11:21 12:2,20 40:19 51:15,16,17 55:10 59:22 63:25 102:16 104:2 106:22 112:22 114:24 118:11 119:12 131:3 133:21 134:7 135:9 160:8 161:13 171:23 177:9 179:4 211:3 212:6 250:4 270:4 274:21,22 275:3 282:10 285:13 287:16 288:6	<b>January</b> 1:6 280:2 318:4 <b>Japanese</b> 103:14 104:20 <b>jargon</b> 273:8 <b>Jasmine</b> 89:7 98:20 100:5 111:22 <b>Jasmine's</b> 111:11 <b>Java</b> 9:8,12,16 <b>JavaScript</b> 26:12,13 26:21 28:9,17 29:16 32:1,7 <b>jaywalkers</b> 117:11 <b>jaywalking</b> 117:12 117:14,22 <b>Jens</b> 188:7 199:4 234:9 240:12 246:21 <b>Jens'</b> 243:12 <b>JO</b> 318:15 <b>job</b> 31:18 58:23 119:15 130:20,23 141:11 177:16 178:2,6,7 212:2 248:5 311:18 313:9 314:5,10 <b>job-related</b> 143:12 146:18 184:1 <b>jobs</b> 94:25 140:18 144:13 178:17,19 178:24	<hr/> <b>K</b> <hr/> <b>Kaifu</b> 199:8 <b>keen</b> 223:13 <b>keep</b> 14:22 25:21,22 27:5 151:6 152:25 196:18 266:1 314:2 <b>keeping</b> 195:6 <b>kept</b> 131:25 <b>Kevin</b> 188:4 235:5 <b>key</b> 8:4 9:24 16:9 19:22 22:15 33:1 51:1,11,15 102:21 112:17 131:3 274:4 304:4,11 305:8 314:16 <b>keys</b> 124:1
<b>interplay</b> 6:4 <b>interpret</b> 41:12,15 315:19	<b>intuitive</b> 152:13 <b>invasive</b> 88:6,9 <b>invest</b> 310:19 <b>invested</b> 175:20 <b>investigate</b> 210:24 261:12 <b>investigated</b> 261:11 315:22 <b>investigating</b> 197:22 200:14 209:19 240:5 262:19 <b>investigation</b> 3:5 4:21 9:13 10:23 14:7 94:12	<b>issued</b> 7:22 8:15 133:21 <b>issues</b> 7:20,23 11:7 11:21 12:2,20 40:19 51:15,16,17 55:10 59:22 63:25 102:16 104:2 106:22 112:22 114:24 118:11 119:12 131:3 133:21 134:7 135:9 160:8 161:13 171:23 177:9 179:4 211:3 212:6 250:4 270:4 274:21,22 275:3 282:10 285:13 287:16 288:6	<b>January</b> 1:6 280:2 318:4 <b>Japanese</b> 103:14 104:20 <b>jargon</b> 273:8 <b>Jasmine</b> 89:7 98:20 100:5 111:22 <b>Jasmine's</b> 111:11 <b>Java</b> 9:8,12,16 <b>JavaScript</b> 26:12,13 26:21 28:9,17 29:16 32:1,7 <b>jaywalkers</b> 117:11 <b>jaywalking</b> 117:12 117:14,22 <b>Jens</b> 188:7 199:4 234:9 240:12 246:21 <b>Jens'</b> 243:12 <b>JO</b> 318:15 <b>job</b> 31:18 58:23 119:15 130:20,23 141:11 177:16 178:2,6,7 212:2 248:5 311:18 313:9 314:5,10 <b>job-related</b> 143:12 146:18 184:1 <b>jobs</b> 94:25 140:18 144:13 178:17,19 178:24	<hr/> <b>K</b> <hr/> <b>Kaifu</b> 199:8 <b>keen</b> 223:13 <b>keep</b> 14:22 25:21,22 27:5 151:6 152:25 196:18 266:1 314:2 <b>keeping</b> 195:6 <b>kept</b> 131:25 <b>Kevin</b> 188:4 235:5 <b>key</b> 8:4 9:24 16:9 19:22 22:15 33:1 51:1,11,15 102:21 112:17 131:3 274:4 304:4,11 305:8 314:16 <b>keys</b> 124:1
<b>interpretable</b> 166:19	<b>intuitive</b> 152:13 <b>invasive</b> 88:6,9 <b>invest</b> 310:19 <b>invested</b> 175:20 <b>investigate</b> 210:24 261:12 <b>investigated</b> 261:11 315:22 <b>investigating</b> 197:22 200:14 209:19 240:5 262:19 <b>investigation</b> 3:5 4:21 9:13 10:23 14:7 94:12	<b>issued</b> 7:22 8:15 133:21 <b>issues</b> 7:20,23 11:7 11:21 12:2,20 40:19 51:15,16,17 55:10 59:22 63:25 102:16 104:2 106:22 112:22 114:24 118:11 119:12 131:3 133:21 134:7 135:9 160:8 161:13 171:23 177:9 179:4 211:3 212:6 250:4 270:4 274:21,22 275:3 282:10 285:13 287:16 288:6	<b>January</b> 1:6 280:2 318:4 <b>Japanese</b> 103:14 104:20 <b>jargon</b> 273:8 <b>Jasmine</b> 89:7 98:20 100:5 111:22 <b>Jasmine's</b> 111:11 <b>Java</b> 9:8,12,16 <b>JavaScript</b> 26:12,13 26:21 28:9,17 29:16 32:1,7 <b>jaywalkers</b> 117:11 <b>jaywalking</b> 117:12 117:14,22 <b>Jens</b> 188:7 199:4 234:9 240:12 246:21 <b>Jens'</b> 243:12 <b>JO</b> 318:15 <b>job</b> 31:18 58:23 119:15 130:20,23 141:11 177:16 178:2,6,7 212:2 248:5 311:18 313:9 314:5,10 <b>job-related</b> 143:12 146:18 184:1 <b>jobs</b> 94:25 140:18 144:13 178:17,19 178:24	<hr/> <b>K</b> <hr/> <b>Kaifu</b> 199:8 <b>keen</b> 223:13 <b>keep</b> 14:22 25:21,22 27:5 151:6 152:25 196:18 266:1 314:2 <b>keeping</b> 195:6 <b>kept</b> 131:25 <b>Kevin</b> 188:4 235:5 <b>key</b> 8:4 9:24 16:9 19:22 22:15 33:1 51:1,11,15 102:21 112:17 131:3 274:4 304:4,11 305:8 314:16 <b>keys</b> 124:1
<b>interpretation</b> 45:25 197:3 276:16 277:8,10,12	<b>intuitive</b> 152:13 <b>invasive</b> 88:6,9 <b>invest</b> 310:19 <b>invested</b> 175:20 <b>investigate</b> 210:24 261:12 <b>investigated</b> 261:11 315:22 <b>investigating</b> 197:22 200:14 209:19 240:5 262:19 <b>investigation</b> 3:5 4:21 9:13 10:23 14:7 94:12	<b>issued</b> 7:22 8:15 133:21 <b>issues</b> 7:20,23 11:7 11:21 12:2,20 40:19 51:15,16,17 55:10 59:22 63:25 102:16 104:2 106:22 112:22 114:24 118:11 119:12 131:3 133:21 134:7 135:9 160:8 161:13 171:23 177:9 179:4 211:3 212:6 250:4 270:4 274:21,22 275:3 282:10 285:13 287:16 288:6	<b>January</b> 1:6 280:2 318:4 <b>Japanese</b> 103:14 104:20 <b>jargon</b> 273:8 <b>Jasmine</b> 89:7	

<b>keyword</b> 158:24	133:16 139:4	123:6,8,11 127:14	304:9,15 305:6	<b>laptop</b> 256:9
<b>keywords</b> 148:7	145:10 146:23	127:20 130:19	306:21,22 307:10	<b>large</b> 17:25 24:9
158:21	150:21 154:25	131:1 138:24	307:15 310:11	27:7 41:18 49:23
<b>kick</b> 5:10 101:25	159:8 161:12	139:20 140:23	311:6,10,14 312:3	50:4,25 63:11 64:6
<b>Kickstarter</b> 258:6	162:11,23,24	141:22 148:5,6,15	312:8,10 315:17	107:14 141:5
<b>kid</b> 58:17,19	163:24 164:16,20	149:1,12,13,18,19	<b>knowing</b> 23:19	148:3 166:12
<b>kids</b> 53:16	164:25 166:5,7,17	149:22,22,22	45:12 267:22	216:16 233:17
<b>kind</b> 23:19,22 24:11	184:11 212:13	150:12,14,16,16	<b>knowledge</b> 24:2	263:12 277:9
30:9 32:3 34:5	224:1,10,12	150:18 151:1,16	36:6,18 44:5,7,12	283:11 294:25
43:9 48:1 57:4	227:10 231:17	152:25 153:6,16	44:17 47:3 50:1,15	<b>large-scale</b> 24:2
62:5 66:7,8 94:14	232:16 269:6	154:12 155:11,16	50:17 81:15 122:8	148:18 150:24
111:2 116:2	299:8 305:21	156:4,6,9,19,21,25	196:25 318:9	157:25 272:5
120:10 124:7,10	<b>Kingdom</b> 108:9	157:1 158:1,12,14	<b>knowledgeable</b>	274:7 281:25
125:19,21,23	<b>kit</b> 163:2	158:15,16,24	36:22 37:19	<b>largely</b> 120:19 311:9
136:6 137:21	<b>knew</b> 4:25 179:10	160:5,7 161:5,7,10	<b>known</b> 22:9,14	<b>larger</b> 49:13 154:12
146:22 153:24	<b>know</b> 4:23 6:13 7:22	161:16,17,21	190:22 199:18	194:11,22 296:16
157:22 160:5,8,13	8:10 14:25 15:1,1	162:3,13,15,17,17	240:9 264:15,22	296:19
160:19,20 161:8	15:2 20:18,19	163:5 165:16	<b>knows</b> 103:7 223:12	<b>largest</b> 22:3,7 220:7
162:2,12 163:9,12	22:12,14,23 23:2,3	167:5,8,9 168:18	263:16	224:7
163:14,23 164:1,4	23:14,15,15 26:15	169:12 174:22	<b>Kristen</b> 13:19 68:5	<b>lasting</b> 71:23 135:17
164:5,17,21,25	27:5,5 28:15,19	175:4,18,22,24	113:15 130:9,18	<b>lastly</b> 31:1 221:13
165:8,10,12,18,20	29:3,24 30:17 31:4	176:7 177:11,17	<b>KU</b> 27:12	259:12
165:24 166:5	33:18 34:22 36:16	177:20 178:3,11		<b>lasts</b> 179:18
167:4,6,10,13,22	38:10 40:19 43:24	179:2,5,11,12	<b>L</b>	<b>late</b> 236:13,18
169:14,17 170:7	43:25 45:8 46:23	180:1,6,8 181:11	<b>lab</b> 74:14 98:12	<b>latest</b> 5:9 113:6
170:24 172:2	47:2 48:4,6,6	181:17 182:4,21	124:16,17	126:16 151:11
174:11,12 175:8,9	50:11,23 51:4	182:25 183:17,17	<b>label</b> 82:8 279:3	271:15
180:9 181:9	53:11,12,13,20	183:21 184:6,18	<b>LabMD</b> 300:16	<b>Laughter</b> 40:24
184:17 185:2,9	54:11,17 57:13,15	185:3,4,11,12,12	<b>laboratory</b> 69:22	<b>law</b> 10:7 34:6 36:20
190:1 193:9	58:1,7 60:2,13	185:24 186:5	<b>laboring</b> 38:18	44:21 60:6 64:8,9
195:12 196:8	61:3,16 62:15,22	199:9,10 203:8	<b>labs</b> 103:6	102:14 110:1,18
197:24 198:1,13	62:23 63:2,3,4,7	209:7 211:2 214:9	<b>lack</b> 44:4,7,17 46:19	119:18 121:21
198:16,19,21	64:5,9,12 65:2,6	219:3 222:20	96:11 150:18	134:2,14,20,21
212:1 213:15	67:13 70:2,14 71:4	224:6 227:1 238:4	180:3 183:1 197:4	141:6 143:6 171:7
222:23 223:13,18	71:15,19,21 73:25	238:5,7,8,13,20	219:8 243:1	218:13 225:17,23
225:7 230:11	74:2,23 75:6,12,20	239:24 241:5	273:21 297:7	228:2,13 276:7
240:8,24 242:14	76:4,22 77:6,17,23	242:13 244:6,19	<b>lacking</b> 171:22	279:16,20 297:24
245:3 247:9 248:7	78:14 79:7,21,25	245:2,4,21,23	301:10 303:18	<b>laws</b> 50:5,12 217:11
252:4,16 253:9	80:6 82:1,2 89:17	253:22 256:3	<b>lacks</b> 20:25	218:10 219:4,5,6,9
259:8 262:17,23	89:20 90:14 92:2,3	257:22 258:2,25	<b>laden</b> 94:23	220:5 221:20
263:12 265:9	100:25 101:6	259:3,4 262:15	<b>land</b> 130:11	226:5 229:15
273:6 275:16	104:7 108:14	263:11 265:14	<b>landline</b> 45:4	234:19 241:6
277:1 279:3,9	117:1,5,7,17,24	266:19 268:6	<b>language</b> 85:6 274:2	<b>laws'</b> 213:19
300:4 303:2,8	118:8,15,16,17,22	270:21 273:10	274:6 278:1 280:6	<b>lawsuit</b> 229:21
307:11 310:18	118:25 119:4,13	276:1 283:15	281:23 310:15	230:10
316:16	119:20,23 120:2,2	284:2 291:16,22	<b>lanyard</b> 3:14	<b>lawsuits</b> 227:18
<b>kinds</b> 24:18 48:20	120:3,6 122:24,25	292:14,24 299:10	<b>LaPlace</b> 195:24	228:21,24,25

<b>lawyer</b> 178:20	120:8 128:17,21	238:23 257:22	<b>limited</b> 132:10	185:5,12 191:13
<b>lawyers</b> 11:3 135:7	132:15 208:17	258:17 284:4	178:5 190:17	209:4 215:17
<b>lay</b> 182:25	210:12 313:25	286:24,25 289:15	191:3 281:17	221:14 231:9
<b>layer</b> 184:16 259:25	<b>leaves</b> 103:18	295:2	286:20 301:3	232:6 233:22
260:13	<b>leaving</b> 130:19	<b>levels</b> 58:17 239:1	<b>limits</b> 47:17 189:10	242:7 243:25
<b>layered</b> 273:17	<b>led</b> 5:11 9:12 195:19	289:8	<b>line</b> 28:17,25 29:16	261:15,18,24
<b>lazy</b> 291:17	268:24	<b>leverage</b> 150:3	40:1 96:1 124:19	262:3 264:7,7,20
<b>lead</b> 7:3 55:15 77:13	<b>left</b> 3:22 125:16	156:1 175:14	150:4 186:22	265:25 266:1,6
136:18 150:19	141:23 193:12	<b>leverages</b> 154:18	216:10 297:12	272:19 298:12,19
168:20 226:9	209:2 248:20	<b>leveraging</b> 277:25	<b>lines</b> 135:4	301:24
229:19 272:7	273:6 275:16	294:3	<b>link</b> 30:18 53:9	<b>Liu</b> 188:13
286:1 300:3	312:14	<b>Lexis</b> 225:17	96:12 98:6 152:18	<b>live</b> 4:13 51:9 58:21
<b>leaders</b> 134:18	<b>left-hand</b> 148:13	<b>liability</b> 224:1	<b>links</b> 17:2 18:18	160:12 180:22
236:11	<b>leftover</b> 145:3	228:14,14 273:1	240:20	<b>live-tweeting</b> 4:16
<b>leading</b> 5:20 11:13	<b>legal</b> 84:25 101:23	301:16	<b>list</b> 70:1 73:18 236:1	<b>lives</b> 47:13 270:17
110:15 131:4	102:10 133:20	<b>Liad</b> 210:9	237:1,18 239:8	<b>living</b> 158:18
<b>leads</b> 42:7 96:19	143:3 181:7	<b>liberal</b> 39:4	253:17	<b>load</b> 265:4,6,19
213:15 312:11	185:11 226:10	<b>libraries</b> 262:8,11	<b>listen</b> 253:22	266:2,4
<b>leaf</b> 50:21	228:6,6,10 272:24	262:15 263:22	<b>listener</b> 253:6	<b>loan</b> 149:17
<b>leak</b> 250:15,17	275:1 301:1,15	269:22 270:2,22	<b>listening</b> 51:22	<b>local</b> 16:20 17:23,24
252:5,16 256:1	310:5 311:4	271:10 297:7	114:15 253:21	18:11 28:7,10
270:18	<b>legalese</b> 94:21 98:9	305:22	<b>Listokin</b> 234:5	183:14 225:15
<b>leakage</b> 270:5 271:5	114:1	<b>library</b> 262:1,4,6	235:5 237:20	228:2
<b>leaked</b> 260:14	<b>legislation</b> 102:9	264:8 271:17	241:2 243:11	<b>locally</b> 18:6
<b>leaking</b> 251:18,20	105:20 108:10	<b>license</b> 54:2 70:13	<b>literal</b> 267:5	<b>location</b> 74:3 76:8,9
251:21 253:14	<b>legit</b> 178:15	<b>lie</b> 65:14	<b>literally</b> 99:10 266:6	76:12,16,18,19
<b>lean</b> 116:22	<b>legitimate</b> 184:12,20	<b>lies</b> 133:18	270:9	77:9 84:4 86:10
<b>learn</b> 48:11,12 70:9	<b>lend</b> 7:2	<b>life</b> 34:14 42:2 43:14	<b>literature</b> 15:22	150:1 162:8
145:9 197:22	<b>lengths</b> 263:23	46:5 51:5 53:2	38:9,12 89:17	180:15 201:18
264:18,19 266:5,6	<b>Leonard</b> 306:24	60:25 76:11 197:8	91:22 210:11	202:2,9 203:2,7,21
266:7,9 267:19,22	<b>lessons</b> 270:20	211:21 213:3	236:3	204:19 256:24
285:6 286:8 302:2	<b>let's</b> 5:10 20:10	215:12 233:6	<b>litigated</b> 229:15	270:5,10 286:24
<b>learned</b> 118:16	24:22 44:19 46:7	<b>lifeblood</b> 200:6	<b>litigating</b> 230:10,10	287:24 292:10
119:9 221:1	117:19,24 135:20	<b>Ligatus</b> 21:16 22:6	<b>litigation</b> 65:5 224:3	313:15
<b>learning</b> 85:6	137:8 152:25	<b>light</b> 117:12 135:14	227:19 228:19,20	<b>locations</b> 25:11
112:23,25 145:6,9	153:1 155:1	150:22 171:9	228:20 229:4,10	26:17 163:17
156:6 160:2	172:15 177:18,25	245:16 255:12	229:19 231:18	<b>lock-in</b> 40:12
164:23 165:7,7	183:19 220:10	256:1 305:25	275:3	<b>locked</b> 128:23
166:6,15 167:2	266:13,14 302:16	310:9 315:23	<b>little</b> 15:25 24:15	<b>log</b> 17:8 73:12
172:25 173:1,8,13	<b>letter</b> 236:10	<b>liked</b> 311:12	26:9 44:20 48:12	118:22
174:4 274:6 278:1	<b>letting</b> 45:15 53:25	<b>likelihood</b> 83:5,12	77:5 90:4 91:4	<b>logarithmic</b> 155:18
281:24 289:9	113:16	84:9 88:20 280:15	93:3,14,15 99:16	156:9
294:3 297:12	<b>Leuven</b> 27:12	<b>Lily</b> 233:5	99:16 120:10	<b>logically</b> 52:16
<b>learns</b> 267:20 268:7	<b>level</b> 30:14 34:9	<b>limit</b> 93:9 272:25	122:10 124:7	<b>login</b> 118:22 254:8
269:4	117:8 131:15	<b>limitations</b> 17:5,10	131:21 137:12,13	<b>logistic</b> 278:9
<b>leave</b> 3:10,16,18,21	144:12 152:13	161:22 176:1	137:19 150:17	<b>long</b> 59:4,9 60:13
5:23 52:2 80:5,9	162:6,9 227:4	220:14	164:18 165:5	81:4 94:19 98:9

106:18 120:25	261:13 262:17	<b>losing</b> 175:10	52:10 54:18 59:25	250:11 259:7
123:20 130:5	265:21 266:13,18	278:15	150:5 208:25	306:19
173:20 186:22,22	269:12 272:14	<b>loss</b> 200:8 223:22,25	<b>low</b> 71:18 205:9	<b>mainstream</b> 32:7
222:7 240:20	274:8,16 275:8	224:3 230:8,9,10	250:24 258:9	55:7 211:3
258:5 273:7 276:6	277:25 282:9	239:9 278:4	<b>low-fat</b> 47:11	<b>maintain</b> 43:8
277:25 285:16	293:11 302:16	<b>losses</b> 230:2,3,9	<b>low-income</b> 8:23	<b>major</b> 38:2,9 107:8
290:17 312:11	304:17 305:4	232:17 239:14	<b>lower</b> 95:24 96:1	<b>majority</b> 12:3 71:16
<b>long-form</b> 91:7,8	313:2 317:3	<b>lost</b> 282:12	99:13 206:15,16	77:15 102:6 109:4
<b>long-term</b> 134:13	<b>looked</b> 21:5 32:9	<b>lot</b> 15:10 17:16	279:12	196:5 226:22
239:9 240:13,17	41:16 45:7 46:16	24:17 25:19 29:21	<b>lowest</b> 266:21	<b>makeup</b> 107:17
<b>longer</b> 56:7 63:1	73:9 83:25 84:2	36:9 39:3,6 41:5	<b>loyalty</b> 12:8 42:19	212:22
124:3 128:1	86:5 87:11,13,18	43:18 44:7 51:16	<b>lucky</b> 177:23 215:1	<b>making</b> 32:15,18,21
214:17 271:4,5	95:7 126:24 136:6	54:9 58:5,19,23	<b>luminosity</b> 256:4	37:21 40:18 54:2
<b>longest</b> 100:9	136:7 167:15	60:15 61:17 62:4	<b>Lunaspae</b> 52:11	54:11 62:14
<b>look</b> 5:7 21:11 24:13	180:1 218:6	66:11,12,21 70:12	<b>lunch</b> 4:6 128:11,14	118:25 119:17,20
26:4,22 27:20	234:24 256:8,10	71:9 103:5 113:24	129:3 130:11	121:19 124:19
28:16,19,23 33:11	270:4 278:17	120:19 121:5,8,20	235:24	140:4 145:20
33:15 35:13 38:9	288:23 315:10	122:7 124:10	<b>lunches</b> 4:4 128:11	181:6 182:1,12
39:12,12,25 40:5	<b>looking</b> 26:15 36:16	137:10 138:11	<b>Lurking</b> 131:9	239:2 246:8
45:1,20 46:4 49:3	38:12 65:11 68:23	142:8 154:12,13		280:22 294:5
54:8 55:9 59:23	72:6 78:14 79:2,21	154:13 155:5,18	<b>M</b>	303:5 311:11
64:16 72:8 78:8	99:18 100:24	156:3 158:10,17	<b>machine</b> 27:3 29:12	315:8
99:15 102:2	102:16 105:19,25	159:23 160:9	85:6 145:6,9 156:5	<b>male</b> 140:16,21
103:20 114:20	108:15 109:2	161:22 166:14,16	160:2 164:23	141:4 143:13
116:18 120:12	111:20 113:20	175:10 180:23	165:6,7 166:6,15	144:2,16,19 145:4
128:6 136:9 155:1	118:20 120:12	189:20,21 190:21	167:2 172:25	145:8,13 168:11
155:2 162:13	124:17,19 126:20	192:25 195:15,19	173:1,8,13 174:3	<b>males</b> 145:1
163:22 164:6	133:1 136:24	196:23 198:3,14	274:6 278:1	<b>malicious</b> 66:14
165:4 170:18	163:14 180:20	211:2 212:10,12	281:24 294:3	253:5 263:24
172:22 177:17	195:11 218:5	232:11 235:14,15	297:12	264:14 265:23
178:15,20,25	229:7 230:20	237:22 240:5	<b>machine-learning</b>	269:12 270:23
179:11 180:3,23	242:9 254:1,25	241:20 242:9,20	275:22,22 280:5	<b>malware</b> 9:11
184:19 189:18	260:11 263:5	242:24 247:25	309:7 315:13	<b>man</b> 178:22
191:16 192:8	274:1 285:13	248:3 250:21	<b>machine-readable</b>	<b>manage</b> 52:18
195:2,9 198:5	287:12 288:9	259:2 261:22,22	273:19 293:12	131:20 285:3
213:19 218:7	304:13	263:3,14 265:2,10	<b>machinery</b> 166:15	297:16
221:15 222:20	<b>looks</b> 27:2 104:1,6	265:16 268:20	<b>machines</b> 27:3,8	<b>management</b> 55:14
223:10,20,25	262:21 265:7	279:10 302:8	<b>macular</b> 211:21	<b>mandate</b> 6:21 113:8
227:9,13,15,18,20	272:19 275:1,11	305:20,24 308:24	<b>mad</b> 52:4	304:10
228:6,19 229:23	306:13	310:19 314:13,17	<b>main</b> 3:22 11:15	<b>mandated</b> 298:25
231:14 232:18	<b>loop</b> 131:17	316:8	16:8 33:2 37:22	<b>Maneesha</b> 130:18
244:19 246:25	<b>lopsided</b> 299:16	<b>lots</b> 70:7,7 71:17	79:1 81:6 82:21	<b>maneuver</b> 304:2
247:22 248:3	<b>Lorrie</b> 13:1 44:8	77:11 174:18	92:15 126:9 131:9	<b>Manne</b> 297:23
249:10 250:3,11	52:25 313:23	182:13 230:1	139:24 153:3	298:8 306:22
253:15,19 254:11	<b>lose</b> 40:23 85:23	235:9 236:22	155:25 202:20	311:2
254:19 258:24	86:3 231:1,3	241:15	206:8 216:9	<b>manner</b> 49:7 239:14
259:5 260:23	232:15	<b>love</b> 15:8 30:16 42:2	217:21 247:15	244:2

<b>manually</b> 84:25	<b>math</b> 284:13	273:5 277:7,14	231:9 234:25	<b>meta</b> 235:21
<b>manufacturer</b> 259:10	<b>mathematics</b> 204:22	279:9 291:12	<b>medians</b> 232:7	<b>metamorphic</b> 244:5
<b>manufacturers</b> 250:21 258:4 259:2,15	<b>matter</b> 101:12 181:7 206:5 248:3 299:7 311:5	<b>meant</b> 213:9 222:22 222:22 308:14	<b>mediated</b> 294:22	<b>method</b> 28:19,23 91:4 156:16
<b>manufacturing</b> 227:25	<b>matters</b> 285:19 301:2	<b>measurable</b> 115:6 115:12	<b>mediates</b> 294:25	<b>methodological</b> 241:1
<b>map</b> 133:2	<b>mature</b> 247:11	<b>measure</b> 17:11 27:18 28:4,15 49:11 82:22 83:10 83:13 84:11 91:21 92:10 116:8 132:6 166:10 180:7 192:10 193:22 216:22 230:20 247:9	<b>medical</b> 6:1 141:19 209:19 213:13,16 220:5	<b>methodologies</b> 171:23
<b>marbles</b> 36:14	<b>maximize</b> 14:20 27:16 208:16	<b>measured</b> 91:25 92:21 192:10 238:25	<b>medication</b> 266:20	<b>methodology</b> 146:14 154:17
<b>mark</b> 275:18	<b>McDonald</b> 44:8	<b>measurement</b> 15:24 16:22 21:19 22:10 25:5,19 29:14 315:9	<b>medicine</b> 210:17 212:20,21	<b>methods</b> 16:19 17:4 27:20 35:6 76:18 90:1 91:5 154:18 156:8 297:13
<b>market</b> 57:22 102:5 120:20 189:2 242:14,20 245:1	<b>McNealy</b> 89:8,11 116:21	<b>measurements</b> 24:3 24:11 26:10 30:23 139:14,16 315:11	<b>meeting</b> 126:14	<b>metric</b> 230:23
<b>marketed</b> 109:19	<b>McQuinn</b> 110:15 113:15 125:18	<b>measures</b> 8:13 16:9 19:22 118:6 143:1 161:21 186:17 248:13 303:19	<b>meetings</b> 305:3	<b>metrics</b> 16:9 19:22
<b>marketers</b> 41:7,20 42:5 43:10 44:5,16 46:2 48:11,12 50:21	<b>mean</b> 6:2 17:10 18:17 37:18 43:1 53:12,23 54:8 58:13,19,23 62:22 66:8,9,23 99:20,22 103:22 104:24 116:23 123:19 124:1 137:22 173:4 174:9,10,15 174:18 179:1,6 183:4,6,16 210:8 230:20 232:4 237:21 245:18 248:4 253:23 254:9 258:4 263:17 298:24 306:12,23 307:21 311:2,16	<b>measuring</b> 115:24 115:25	<b>Mellon</b> 80:13 136:18 199:6 272:1 282:23 313:24	<b>Michael</b> 136:16,17 136:21 147:19 177:10
<b>marketers'</b> 41:14 47:18,21 48:23	<b>meaning</b> 48:15 142:25 165:23 173:9 270:1	<b>Mechanical</b> 84:19 276:8	<b>member</b> 4:21 148:23 149:6 267:23	<b>Michael's</b> 172:3
<b>marketing</b> 39:21 50:12 107:22,23 243:3	<b>meaningful</b> 55:21 96:22 97:10 98:15 99:7 124:2	<b>mechanism</b> 21:9 56:1 160:17 201:16 202:4,19 220:20	<b>members</b> 63:17 212:9	<b>Michigan</b> 110:17
<b>marketplace</b> 5:25 10:15 11:5,24 32:12,19,21 33:5 37:25 39:11 57:18 102:5 242:22 243:9,13	<b>means</b> 16:25 17:1 39:13,14 40:12 42:24 55:10 60:24 62:7 64:8 102:8 104:4 202:14 205:9,10 211:21 244:19 253:13 257:16 258:16	<b>mechanisms</b> 16:6 21:6 55:20 56:23 56:23 154:25 156:20 186:12 248:14 264:1 310:16	<b>memories</b> 250:25	<b>microeconomics</b> 199:13 236:19
<b>markets</b> 121:15		<b>media</b> 56:16 90:24 92:4 97:2 149:19 264:23	<b>men</b> 91:10,16 140:24 141:12 169:15,25 177:16 179:2 180:8 181:15 182:5 186:5	<b>Microsoft</b> 57:20 160:3 165:18 176:12 295:7
<b>Marotta</b> 199:5 200:23 248:21,23		<b>median</b> 230:22	<b>mental</b> 75:12 122:7 122:12 123:5,17	<b>middle</b> 51:13 138:16 261:25 302:10,21 303:7 308:8
<b>Mason</b> 171:6 183:22 234:6			<b>mention</b> 57:22 122:6	<b>Miller</b> 210:24
<b>massive</b> 306:3 307:4			<b>mentioned</b> 83:23 88:23 97:6 98:20 99:2 109:18 156:22 170:13 214:17 276:25 285:15 299:20 306:11	<b>million</b> 10:18 26:11 75:9 77:6 158:1 174:19 230:17,18 230:24 231:12,12 232:3,4 288:25
<b>mastectomy</b> 213:11			<b>menu</b> 178:19	<b>million-site</b> 24:10
<b>master's</b> 171:19			<b>menus</b> 293:9	<b>millions</b> 10:2 79:22 175:21
<b>MasterCard</b> 232:20			<b>merely</b> 17:13 35:20 298:22	<b>mind</b> 3:12 115:13 116:4 148:22 154:4,5 196:18 284:18
<b>match</b> 81:17,22 210:4			<b>message</b> 303:16	<b>minds</b> 33:23
<b>matching</b> 112:2 205:24			<b>messages</b> 69:13	<b>mine</b> 53:8
<b>material</b> 94:23 210:7 219:21			<b>met</b> 48:3 90:11	<b>Mingyi</b> 188:12
<b>materials</b> 4:14 125:6				<b>minimum</b> 195:25 238:22,23,25

<b>Ministry</b> 214:19	32:19 38:17 62:8	<b>money</b> 44:2 213:1	<b>movement</b> 270:13	<b>near</b> 72:21 178:17
<b>minutes</b> 14:22 68:12	64:20 78:7 96:7	231:1 247:5	<b>moves</b> 13:12 119:18	<b>nearby</b> 76:16
110:14 142:17	122:20 123:17	259:11 261:1	119:19 127:2,3	266:21
157:1 186:23	131:11 146:1	262:9 310:20	<b>movies</b> 183:21	<b>nearly</b> 12:7 14:15
218:25 298:6	183:18 191:1,3	<b>monitor</b> 16:9 19:22	<b>moving</b> 35:13 116:6	<b>necessarily</b> 106:21
<b>misaligned</b> 208:14	192:1,1,24 196:8	45:14 151:5	116:17 117:19	114:5,11,16 121:2
<b>misconceptions</b>	198:8,8,11 200:22	<b>monitored</b> 256:8	126:5,6	175:8 178:5
37:16 38:19 50:7	201:9 202:20	<b>monitoring</b> 254:4	<b>Mozilla</b> 23:7	179:11 194:14
<b>misleading</b> 123:11	203:16 204:22,24	<b>month</b> 9:6 280:3	<b>Mulligan</b> 143:7	209:6 263:20
<b>misled</b> 39:24 57:4	205:16 206:2,9,21	<b>monthly</b> 24:10	171:7,16 180:11	292:21 310:9
<b>mismatch</b> 85:14,14	234:12 235:18	26:10	180:17 183:7,10	<b>necessary</b> 30:13
85:15,17,23 86:16	251:5 257:10	<b>months</b> 22:10 31:4	<b>multi-dimensional</b>	200:8
86:18,22,23 87:8	286:13 289:25	53:2 60:7 184:9	246:19	<b>necessity</b> 51:18
87:14,22 88:8,9,12	303:4,7 309:6,12	196:1	<b>multi-stage</b> 201:8	<b>need</b> 6:13,18 8:10
<b>mismatched</b> 80:13	<b>modeled</b> 103:2	<b>MoPub</b> 269:22	<b>multiple</b> 25:13,14	10:8 11:21 29:18
80:17 82:11,13	<b>modeling</b> 201:8,18	270:9	82:25 83:2 172:5	29:19,19 40:5
88:24	274:8 283:3	<b>Morgan</b> 230:25	231:17,22 258:4	56:23 60:14,16
<b>mismatches</b> 82:23	<b>models</b> 64:16 75:12	<b>Moriarty</b> 188:3,4	262:8,11,11	63:9,11,21 67:4,6
83:20 85:13 86:16	122:7,12,14,16	199:4 210:15	265:12 275:25	70:14 79:10
87:7,25 88:6,10	123:5 198:7	222:3 233:25	279:2	108:19 110:5,7
112:3	236:17,18,21	246:21 248:19,22	<b>multiply</b> 6:7	113:6,21 119:13
<b>mission</b> 11:9 134:24	275:22 278:9	249:7	<b>mutation</b> 213:8	120:5,11 127:22
<b>mistakenly</b> 8:24	280:6 294:4,12	<b>morning</b> 3:3 5:17		131:5 145:21
<b>MIT</b> 210:16 211:25	295:20 305:17,24	7:12 11:25 14:3	<b>N</b>	155:17 156:3
<b>mitigation</b> 183:4	315:21	31:13 68:4 89:11	<b>N</b> 2:1 3:1 318:1,17	162:22 170:22
<b>mitigations</b> 266:23	<b>moderately</b> 195:6	128:10 132:25	<b>name</b> 15:14 188:4	172:19,20,21,24
<b>mixed</b> 90:1	<b>modern</b> 60:5 236:22	142:22 275:6	266:9 267:14,16	172:25 173:16
<b>mobile</b> 3:8 7:25,25	260:24 262:7	281:3 285:12	267:21 268:2,7	174:3 175:14
8:1 10:24 43:6	<b>modest</b> 19:14	<b>morphed</b> 125:19	269:15	179:6 185:10
60:14 68:25 73:7	<b>modified</b> 291:9,13	<b>motion</b> 254:5	<b>name-and-shame</b>	186:9 201:25
250:19 260:22,22	<b>modify</b> 286:1	<b>motivate</b> 148:3	62:19	203:1,8 237:3
261:5,14,16,18,24	290:20	286:4	<b>names</b> 269:8,9	238:8,14,21
262:1,15 263:22	<b>modifying</b> 291:22	<b>motivating</b> 137:8	<b>naming</b> 51:20	244:23 261:14
264:21 265:17,17	309:22 310:10	291:1	<b>narrow</b> 87:2	262:17 264:21,23
265:24 266:5,14	<b>modulate</b> 243:20	<b>motivation</b> 80:18	<b>narrowing</b> 119:22	265:2 267:3
266:15 267:18,19	<b>moment</b> 74:25	81:6 189:5 222:13	<b>Nathan</b> 19:24	268:18 277:7
269:6,7,17 270:1	107:23 121:10	223:11	<b>national</b> 41:10	282:15 289:11
270:12,12,23,24	126:8 130:15	<b>motivations</b> 199:17	215:2 225:15	293:18 294:11
271:4 274:3 283:8	140:9 244:8	222:13 223:20	<b>natives</b> 37:8,10	295:8 299:1,3
283:17 284:20,22	281:18 282:2	291:7	<b>natural</b> 85:5 153:20	308:15,18 311:16
286:14 288:9	310:22	<b>motivators</b> 95:13	274:2,6 278:1	311:17 315:1,18
291:6 292:2	<b>Monday</b> 313:23	<b>mouse</b> 10:3	280:5 281:23	317:1
294:24 296:2,3	<b>monetary</b> 194:14	<b>move</b> 51:25 56:12	284:20	<b>needed</b> 30:20 127:2
304:18 305:1,16	196:12,13	64:19 97:13	<b>naturally</b> 135:13	155:5,11,12 271:6
306:3,7 313:8	<b>monetization</b> 126:7	116:11 126:10,20	<b>nature</b> 100:21 121:5	316:13
<b>Mobiquity</b> 42:12	<b>monetized</b> 126:17	126:21 295:8	140:25 299:6	<b>needs</b> 18:6 107:4
<b>model</b> 32:15,17,17	<b>monetizing</b> 126:22	<b>moved</b> 93:17 102:17	<b>navigate</b> 6:3 49:1	123:7 268:6

308:16	235:19 237:5	235:6 300:18	<b>nudges</b> 290:22,23	190:16 191:8
<b>nefarious</b> 161:19	243:9 244:18	<b>noted</b> 91:1 95:6,17	291:3,14,17,20	194:20 198:20
<b>negative</b> 94:9,10	258:18 297:16,19	95:18 98:8 106:2	303:8	226:6 239:20,23
96:3 212:4 215:15	313:22	106:15 108:4	<b>nudging</b> 303:6	240:3
217:15 219:1,16	<b>newest</b> 57:14	125:11,12 181:13	<b>number</b> 8:16 10:1	<b>observed</b> 33:16 79:1
221:18 241:21	<b>news</b> 21:23,24 22:2	204:3 316:12	18:19 19:3 24:9	145:7 188:23
<b>negatively</b> 217:11	22:18 53:9 92:4	<b>notes</b> 314:12,14	34:25 36:10 57:22	194:15 196:4
<b>negligence</b> 102:11	97:2 196:23	318:7	137:21 151:8	225:23 315:15
228:12,14	219:25 220:1,3,4	<b>notice</b> 3:25 32:13,16	155:12,18,19	<b>observers</b> 41:12,23
<b>neither</b> 53:12	221:5,15 225:15	40:7 54:24 69:3,12	158:23,25 167:22	<b>observes</b> 203:20
128:16	242:23 264:11	71:10,12 76:23	188:20 190:16	<b>observing</b> 229:21
<b>nerdy</b> 289:6	276:20 288:1	77:5 80:6,8 81:24	193:20 194:22	<b>obtained</b> 204:23
<b>nervous</b> 241:24	<b>newspaper</b> 137:24	82:1,4,5 87:18,19	200:3 208:20	<b>obvious</b> 17:22 20:17
<b>Nest</b> 252:13 255:4	<b>newspaper's</b> 141:20	87:25 88:14 96:22	223:24 227:11,13	20:24 107:22
255:15 256:10,12	<b>nice</b> 173:25 178:13	107:1 109:13	227:17,23 228:20	114:25
256:18,24	209:14 213:21	111:10 120:6	229:18 248:24	<b>obviously</b> 76:24
<b>Netflix</b> 150:5	214:2,22 224:8	122:22 123:1,10	277:9 289:10,17	77:5,25 151:15
<b>Netscape</b> 188:19	241:12 270:13	125:12 131:10	290:14 291:19	174:9 213:12
<b>network</b> 40:13	273:4 280:4	229:9 245:20,20	292:15 294:7,12	284:18 300:21
76:16 160:23	<b>night</b> 94:22 97:6	280:22 294:5	295:1,4 314:25	<b>occur</b> 55:20 56:21
250:13 251:17,25	<b>nirvana</b> 43:16	300:9 309:1 313:5	<b>numbers</b> 45:23	65:5 225:20
252:8,11,17 253:3	<b>Nissenbaum</b> 115:11	315:5	101:4 143:13	231:19
253:5,15,18 254:1	<b>no/yes</b> 85:14,23	<b>noticed</b> 111:9	216:17 232:23	<b>occurred</b> 74:15
254:11,21 256:2,7	86:22 88:8	<b>notices</b> 81:21 82:9	<b>numerosity</b> 239:6	<b>occurring</b> 64:4
259:13,23,25	<b>noise</b> 154:14	82:16 87:17 88:17	<b>numerous</b> 93:13,19	76:21 77:24
260:6,12,15 261:5	<b>noisy</b> 195:21	88:24 112:18	<b>nutrition</b> 82:7	229:22
<b>network-level</b> 312:2	<b>Nomorobo</b> 10:15,16	233:9 274:10,19	<b>NYU</b> 15:6	<b>occurs</b> 3:17,20
<b>networking</b> 28:8	<b>nonprivacy</b> 82:24	274:23 308:19,22		70:11,16 102:4
<b>networks</b> 200:21	<b>nonprofit</b> 102:25	308:25 314:25	<b>O</b>	<b>oddy</b> 45:20
208:23 286:17,18	<b>nonrepeat</b> 232:6	<b>noticing</b> 54:23	<b>O</b> 3:1 318:1,1,1,17	<b>OECD</b> 214:12
<b>never</b> 20:3 21:5 35:9	<b>nonspecific</b> 105:4	<b>notification</b> 226:5	318:17,17,17	<b>offender</b> 283:21
47:4 64:23 70:4	<b>nonstandard</b> 254:22	229:15 230:6	<b>obfuscation</b> 51:16	<b>offer</b> 46:10 106:1
73:1 76:14 153:22	258:12	233:8 313:14	<b>object</b> 18:5 287:25	132:21 135:5
175:12 245:9	<b>nonstop</b> 5:8	<b>notifications</b> 233:15	<b>objects</b> 16:20 17:23	194:10 217:16
304:8	<b>normal</b> 74:11	<b>notify</b> 109:10	<b>obscure</b> 149:11	235:4 273:9
<b>nevertheless</b> 141:11	<b>normally</b> 107:12	<b>notion</b> 42:1,7 61:5	<b>obscurity</b> 56:5	281:11,13
143:20 202:25	224:17	61:15 115:10	150:18	<b>offered</b> 12:8 234:10
243:8 271:1	<b>Norman</b> 272:6	231:15 245:23	<b>observable</b> 127:20	234:25 316:5
<b>new</b> 5:24 10:8 11:4	282:22,22 297:15	<b>notions</b> 41:8 142:15	<b>observation</b> 17:22	<b>offering</b> 42:22 132:8
12:25 17:24 20:10	306:10 307:2	<b>notorious</b> 246:22	146:20 242:18	217:7 221:12
26:2 29:7,7 51:12	309:15	<b>novel</b> 236:13	<b>observations</b> 145:10	<b>offers</b> 242:21,23
57:12 58:5 120:18	<b>Norman's</b> 300:21	<b>NSF</b> 272:5	153:19 154:8	243:9,13
125:24 126:21	<b>normatives</b> 238:2	<b>nuance</b> 145:18	156:3 157:18	<b>Office</b> 3:5 4:20
134:16 150:21	<b>norms</b> 56:14	<b>nuanced</b> 79:2 127:4	224:5	10:22 14:6 121:13
162:23 199:24	<b>note</b> 82:20 85:12	142:18 249:2	<b>Observatory</b> 157:11	<b>office's</b> 11:2
209:10,11 220:24	91:10,16 93:4,4	<b>nuances</b> 143:8 277:2	157:15,20	<b>officer</b> 246:23
223:22 225:15	96:13 185:1 205:9	<b>nudge</b> 290:20	<b>observe</b> 153:17	<b>offline</b> 37:13 89:12

89:18 90:5,11,15 91:3 <b>offload</b> 259:24 260:12 <b>oftentimes</b> 248:7 <b>oh</b> 28:15 61:9 62:6 70:13 94:4 119:6 172:20 180:21 183:24 216:19 276:2 <b>Ohlhausen</b> 66:20 <b>oil</b> 199:24 209:10,11 237:5 <b>okay</b> 41:19,25 44:22 45:16 46:13 48:13 101:1,10 102:11 103:8,25 125:15 159:21 161:20,24 186:18 210:19 232:11 238:14 241:12 258:20 266:10 267:9 270:20 276:3 303:25 <b>old</b> 305:16 <b>older</b> 9:8,12,16 <b>oligopolies</b> 209:22 <b>Omer</b> 15:5 <b>Omer's</b> 38:25 <b>once</b> 12:15 66:6 72:25 82:13 83:18 169:21 195:15 202:16 214:17 279:2 280:21 296:8 310:7 311:14 <b>one-size-fits-all</b> 79:7 <b>one-week</b> 75:8 <b>ones</b> 77:24 91:24 96:25 99:4 159:1 164:9 178:12 247:12 256:12 258:5,5 307:7 <b>ongoing</b> 107:14 120:23 173:15 176:12 185:16 <b>online</b> 2:10 5:24	11:19 14:10 15:16 15:20,25 16:5,6,10 16:12,15,16 17:11 18:21 19:1,5,23 32:5,15 36:21,23 36:24 37:12 41:21 42:8 45:13,14 48:5 51:6 52:8 69:16 80:14,17,19,20 81:7 84:17 89:12 89:13,16,19 90:5 91:3 92:13,14,19 93:15 95:13 96:16 102:6 103:11 105:15 106:5 107:1 108:7 111:8 119:16 123:6 136:24 137:18 138:25 140:1 142:3 151:2 155:9 157:11 160:12 200:8 201:5,9,18 201:24 203:18 219:2 235:11 271:20 281:19 <b>opaque</b> 138:24 139:4 148:4 <b>open</b> 4:3 30:18 72:5 116:19 130:13 132:15 141:23,23 146:8 147:8,9 152:8 170:19 184:3 186:16,21 295:9,9 296:11,14 303:23 305:10 306:12 307:3,5 <b>opened</b> 195:15 <b>opening</b> 53:10 195:18 296:20 304:8 <b>OpenWPA</b> 16:22 <b>OpenWPM</b> 24:7,16 24:20 26:25 29:14 29:17 <b>operate</b> 32:12 56:1 166:1 189:7 190:14 244:15	287:21 292:22 <b>operated</b> 140:8 <b>operates</b> 140:5 189:2 <b>operating</b> 73:10 75:25 76:10 105:20 289:5 <b>operators</b> 82:17 305:22 309:21 <b>opinion</b> 38:9 55:18 175:1 186:8 <b>opportunities</b> 8:24 181:3,4,7,21 305:4 <b>opportunity</b> 6:22 13:14 77:16 98:14 99:7 100:13 104:7 104:8 125:16 <b>opposed</b> 76:13 90:17 103:1 225:6 226:18 <b>opposing</b> 197:2 <b>opposite</b> 47:25 196:9 <b>opt</b> 99:24 124:25 <b>opt-out</b> 61:19,21 <b>opt-outs</b> 61:18 <b>opted</b> 61:23 <b>optimal</b> 307:11 <b>optimism</b> 243:14 <b>optimistic</b> 44:23 <b>optimize</b> 145:11 <b>opting</b> 55:7 <b>option</b> 62:13 <b>options</b> 12:23 <b>Oracle</b> 9:7,15 246:23 <b>order</b> 9:14 43:8 70:15 98:2 113:7 125:5 148:6 149:16 155:3 156:3 157:16 164:23 170:24 175:15 185:10,12 195:1,21 201:7 208:16 222:15 237:2 238:6 261:13 262:16	267:23 296:6 315:15 316:12 <b>ordered</b> 252:9 <b>orders</b> 109:23 <b>ordinary</b> 37:24 115:3,5 121:2 <b>Oregon</b> 89:7 <b>organic</b> 39:11,12,13 44:1 232:22 <b>organization</b> 131:4 189:23 247:20 <b>organizations</b> 42:14 189:14,17 190:21 192:16 195:3 197:5 198:13,15 <b>organize</b> 288:3,10 <b>organized</b> 131:1,3 <b>organizers</b> 13:18 221:25 <b>organizing</b> 314:5 <b>orientation</b> 158:8 <b>origin</b> 264:15 <b>original</b> 5:21 <b>originally</b> 14:16 272:15 <b>Oscar</b> 36:5 <b>OTech</b> 3:6 10:23,23 11:5 13:18 <b>other's</b> 113:1 265:14 <b>Ottenheimer</b> 298:1 301:21 307:14 309:2 <b>outage</b> 224:22 <b>outcome</b> 182:14 183:3,12,13,13 204:3,6,25 312:7 <b>outcomes</b> 8:19 172:16,19 174:1 182:9 213:17 217:23 221:18 299:13 <b>Outgoing</b> 256:21 <b>outlaw</b> 287:21 <b>outline</b> 273:12 <b>outlined</b> 8:16 279:18 312:18 <b>outlook</b> 34:14	<b>output</b> 80:3 162:19 163:12,25 164:22 172:6 <b>outputs</b> 151:23 152:15 162:3,12 163:15,19,23 166:8 <b>outreach</b> 123:7 <b>outright</b> 123:11 <b>outside</b> 4:5,9 54:3 128:12 131:18 133:7 145:24 173:24 253:4 255:10 258:14 260:14 305:23 <b>outsider</b> 160:1 <b>outstanding</b> 136:12 <b>ovarian</b> 213:10 215:9 <b>over-saturated</b> 94:24 <b>overall</b> 17:9 42:14 157:25 193:23 195:8,22 197:15 198:22 226:12,20 229:4 297:19 301:8 <b>overbid</b> 206:19 <b>overblown</b> 231:13 <b>overcoming</b> 273:16 <b>overflow</b> 4:5,6 128:14 <b>overgeneral</b> 312:1 <b>overgeneralization</b> 311:24 <b>overlapping</b> 27:16 <b>override</b> 31:24 32:8 <b>oversight</b> 101:22 150:19 159:7 <b>overview</b> 69:1 193:9 272:13 <b>overwhelmed</b> 71:11 <b>overwhelming</b> 77:21 <b>overwhelmingly</b> 108:17 <b>owned</b> 263:11
---	---	---	--	---

271:14 292:21,23 292:23 293:1 <b>owners</b> 292:8,12 293:3 294:15 <b>Oxford</b> 100:7 <b>Oz</b> 58:18	210:9 212:11 215:19 216:7 219:21 236:1 249:7 264:3 269:19 271:20 300:21 306:24 311:21 <b>papers</b> 42:18,18 115:8,9,15 116:2 174:11,12 177:11 182:23 198:4 235:9,16,19,20 242:11 298:9,10 298:13,15 299:8,9 299:10,25 300:10 300:19 301:8 <b>paradox</b> 42:1,5 <b>paragraph</b> 278:25 280:10,11,14 <b>paragraphs</b> 278:7 278:11,18,24 280:14,16,18 <b>paralegal</b> 3:4 <b>parallel</b> 217:13 <b>parameters</b> 205:17 206:2,10,21 <b>Paris</b> 214:18 <b>parity</b> 162:12,14 <b>part</b> 9:9 10:11 27:11 30:6 35:10 38:2 58:5,23 59:2 70:13 74:3 79:15 84:22 88:18 119:11 123:16 143:7 166:3,4 183:22 184:6 194:1 207:22 219:7 222:16 233:11 248:15 259:13 275:1 276:22 296:15 313:6 <b>Parthenon</b> 36:13 <b>participant</b> 92:17 <b>participants</b> 5:7 13:15 77:15 79:4 84:19 91:7,15 92:1 92:11 95:6 197:24	248:16 <b>participate</b> 75:7 90:18 105:1 190:20 191:6 192:25 193:5 294:17 <b>participating</b> 3:13 193:11 196:17,18 198:15 246:14 248:18 249:12 314:11 <b>participation</b> 106:13 190:15 191:2,3 196:8 198:7,12 247:3,4 <b>particular</b> 13:19 21:6 31:15 47:12 70:24,24 74:22,24 93:11,20 97:12 102:10 107:24 121:12 125:1,7 132:11 145:2,8 147:5 156:8,20 158:5 162:18 172:2 173:12 181:9,12 182:14 184:4,11 189:25 191:9 192:4,9 193:21,24 195:7 197:20 215:23 241:8 248:8 251:7 252:11 266:7,9,20 266:22,23 267:3 267:14,21 268:9 269:18 271:13 277:22 279:8 283:7,9 285:6,14 294:3 <b>particularly</b> 117:10 117:15 173:2 221:4 <b>particulars</b> 45:8 <b>parties</b> 20:12 22:23 35:22 51:13 110:3 112:6 127:10 149:25 165:15 262:23	<b>partly</b> 106:17 142:21 311:25 <b>partner</b> 316:11,15 <b>parts</b> 166:2 199:25 260:4 272:14 276:25 278:19,19 278:21 <b>party</b> 18:13 23:24 25:4 82:18 225:22 292:24 <b>party's</b> 10:1 <b>passive</b> 253:6 <b>password</b> 101:9 254:9 <b>patch</b> 27:19 29:15 258:22 <b>patching</b> 133:17 259:12 <b>path</b> 256:3 <b>paths</b> 315:7 <b>pathway</b> 43:15 <b>patient</b> 101:20,21 102:1 167:7,12,19 168:4 216:5 219:17 220:18 <b>patients</b> 167:6 168:11,25 217:6 217:17,24 218:3 221:10,11,23 <b>pattern</b> 310:7 <b>patterns</b> 224:10 <b>Paulson</b> 236:14 <b>pay</b> 181:16 183:24 193:14 194:2,17 194:18 200:9 202:12 247:6 <b>paying</b> 33:24 193:13 238:13 <b>payment</b> 203:5 204:18 232:19 <b>pays</b> 202:15 259:12 <b>PCP</b> 39:22 <b>pedigree</b> 236:15 <b>peer</b> 94:12,13,15 96:5 215:3 <b>Peng</b> 188:12 <b>Penn</b> 44:21 52:3	188:7,14 <b>Pennsylvania</b> 41:3 <b>people</b> 4:25 14:18 15:16 16:6 20:13 22:11,14,21,25,25 23:7 27:12 29:23 30:1,17,22,24 31:22 32:21 33:4 33:14,15,18,23,25 34:11 35:5,15,16 35:24 36:4,7,17,21 36:23,24 37:2,4,8 38:3,18 41:16,24 42:1,1,6 43:25 44:9,17,24 45:21 46:17,19,23 47:7 47:19,22 48:3,8,13 48:24 49:5,6,13,16 49:24 50:13,23 51:6,6,19 53:18 54:16 56:3 57:22 57:23 59:12,13 62:15 65:22 66:12 69:22,24,25 70:6 70:11,12 71:11 73:14,25 74:9 75:7 75:8 76:3,20 77:23 78:4 79:6,8,17 80:8 89:17 93:12 93:14,25 96:3,10 97:25 98:13 99:11 99:16 103:17 104:22 106:15,16 114:1 117:17,21 118:6,7,17 119:3 119:23 120:16 121:22 123:4 125:12 127:3,5,10 127:16,25 130:19 130:21 136:25 137:1 138:2 139:9 144:12 146:1 147:14,15 149:22 161:2,20 169:9 171:21 172:12,17 172:20 173:21,25 177:25 178:2,22
--	--	---	--	---

179:17 180:22 181:16 182:3,6 183:8,20,20 184:18 185:8 199:11,19 215:4 215:21 216:13,15 220:8 221:4,8,21 222:24 237:12 239:12 241:20 249:9 252:8 258:6 258:22,24 261:11 263:15 264:24,24 266:18 272:8 276:3,9 282:25 283:14,15,24 284:3,14,16 286:13,21 287:6 287:24 288:4,5,21 289:9 290:8,25 291:24 292:12,15 292:22 293:9 295:10 296:20 299:8 302:9,17,23 302:24 303:1,6 304:13,19 305:4 307:24,25 309:8 309:12 315:11 316:12 <b>people's</b> 37:16 45:7 108:18 124:17 214:25 283:3 294:4 <b>per-user</b> 79:11 <b>perceive</b> 12:5 239:12 <b>perceived</b> 92:11 104:14,15,23,23 105:16 <b>percent</b> 18:10,14,24 18:24 22:5 35:3 37:6,7 45:12,16,19 45:22 46:2,10,11 46:15,17 47:12,15 47:20,21 48:13 49:8,10 50:3 75:16 75:19 76:7 78:11 78:19,24 88:2,12	103:17,19 104:15 104:19,20,20 109:5,8,9,9 111:17 111:19 141:5 152:11 167:19 191:11 192:15 194:15 212:23 213:14 215:18 229:8,11 231:21 232:1,24,24,25 233:1,2 268:7 277:6 283:23 288:15 289:16,18 291:13 <b>percentage</b> 18:23 46:21 49:13,24 109:7 207:19 227:16 229:18 232:23 233:16 277:16 <b>percentages</b> 50:4 <b>perceptions</b> 11:23 122:18 241:23 <b>Perfect</b> 21:15 <b>perfectly</b> 224:16 <b>perform</b> 223:14 <b>performance</b> 76:10 161:15 276:4,5 277:3 <b>performed</b> 73:8 <b>performers</b> 37:11 <b>performing</b> 152:16 <b>perilous</b> 299:16 <b>period</b> 11:17 15:5 52:1 75:8 193:24 290:18 <b>periodically</b> 157:21 <b>permission</b> 69:3,7 69:18 71:1,2 75:10 104:4,6,10,12,22 105:3 288:9,16 289:3 305:17,24 <b>permission-based</b> 105:2 <b>permissions</b> 68:19 71:16 111:18 284:12,12 289:21	<b>permitted</b> 128:15 <b>persist</b> 18:8 <b>persistent</b> 21:6 212:8 <b>person</b> 4:25 42:12 77:8 90:11,16 109:10 118:3 179:23 211:10 214:18 253:20 257:21 266:24 267:2 268:8 <b>person's</b> 107:16 <b>personal</b> 6:12 12:11 35:21 38:4,5 39:18 40:9 42:23 43:14 47:19,22 50:15 59:16 60:4,15,16 78:4 100:19,24 107:10,15 112:6 120:25 151:19 199:11,24 200:1,5 200:10 213:3 224:18,24 252:4 297:17 <b>personalization</b> 43:10,15 60:19 142:3 151:21 <b>personalized</b> 50:23 210:17 212:20,21 283:6 285:1,5,22 286:3 289:8 290:9 291:5 293:15,21 294:4 295:11,16 295:19 296:9 312:20 <b>personally</b> 59:15,25 <b>personnel</b> 239:6 <b>perspective</b> 61:2 102:20 103:23 111:15 118:5,8 160:6,7,16 189:17 247:14,16 261:15 265:15 <b>perspectives</b> 274:25 <b>pertaining</b> 197:20 <b>pertains</b> 285:20 <b>pervasive</b> 268:10	<b>pervasively</b> 15:17 <b>pessimistic</b> 258:1 <b>PETs</b> 243:15,16,24 <b>Pew</b> 11:25 41:22 <b>Ph.D</b> 250:6 <b>pharmacists</b> 266:19 <b>pharmacy</b> 266:20 267:11 268:13,15 <b>phenomena</b> 159:8 184:4 <b>Phillips</b> 100:7 105:24 120:9 126:3 <b>philosophy</b> 39:3 45:7 <b>phished</b> 263:18 <b>phishing</b> 50:3 224:25 226:19 <b>phone</b> 10:1 43:6 57:14 58:18 59:9 73:20 74:2,22 75:21 77:12 251:5 261:6,7 262:25 263:1 264:13,18 264:19,22 284:8,9 284:10,17 294:25 <b>phones</b> 3:9 73:13,14 74:9,11 251:2 283:17 289:12 290:6,13 <b>photo</b> 90:13 252:12 252:18,19 253:7 253:13,16,21,23 <b>photographs</b> 252:24 <b>photos</b> 90:11,16,19 160:23 <b>physical</b> 40:8 45:13 54:1 166:8 <b>physiological</b> 124:17 <b>PI</b> 272:7 <b>pick</b> 53:16 114:6,7 252:17 <b>picked</b> 36:9 242:21 242:25 243:10 254:2 <b>picture</b> 45:18 46:14	56:5 57:3 131:7 209:1 227:14 262:24 267:4,5,6,7 270:7,8 279:22 305:15 <b>pictures</b> 56:4 161:3 207:3 <b>pie</b> 207:17,21,22 <b>piece</b> 143:5 215:13 236:9 262:3,4 <b>pieces</b> 119:17 134:10 137:12,13 137:14,19 142:20 173:11 186:13 203:18 204:13 <b>piggy-back</b> 236:9 <b>pill</b> 267:4 <b>piloted</b> 290:5 <b>pinpoint</b> 98:18 180:7 <b>pitch</b> 40:18 211:4 <b>Pittsburgh</b> 144:8 <b>Pixel</b> 21:14 <b>PixStar</b> 252:18 <b>place</b> 10:2 42:6 45:3 47:8 63:20 66:25 117:22 124:8 137:20 196:13 197:24 <b>placed</b> 17:18,19,19 18:17 152:19 <b>placement</b> 153:12 <b>places</b> 57:23 59:10 103:6,8 247:21 300:5 <b>plaintiffs</b> 228:17 <b>plan</b> 83:13 <b>planning</b> 88:18 208:21 <b>plate</b> 54:2 <b>platform</b> 16:22 25:9 84:20 190:2,20 191:4,9 193:23 234:15 305:22 313:8 <b>platforms</b> 68:25 73:7 135:17
--	---	--	---	---

188:24 189:16 190:11,14 191:5 192:4,24 201:6 234:13 248:12 <b>play</b> 57:3,6 58:1 197:11 245:5 253:1 266:17 272:20 304:3 <b>played</b> 9:19 201:14 <b>player</b> 207:20 <b>players</b> 201:12,20 201:25 202:21 203:16 207:5,16 208:13 231:14,21 232:2,5,6,9 243:1 244:18 273:5 294:20 295:4,6 296:19 305:15 <b>plays</b> 14:25 203:9 311:1 <b>please</b> 3:8,12,15,23 3:25 46:6 68:3 128:18 248:22 <b>pleased</b> 130:3 136:11 221:19 <b>pleasure</b> 130:12 <b>plenty</b> 216:7 <b>plotted</b> 191:19 <b>plug-in</b> 281:15,20 <b>plugin</b> 82:19 <b>plus</b> 26:20 29:10 30:4 144:13 178:13 <b>point</b> 22:8,15 23:12 29:13 33:1 37:22 41:14 44:23 54:15 56:19 57:25 66:9 67:6 124:24 176:3 178:3 179:24 181:19 182:20 183:1,10 185:15 196:22 197:12 203:17 235:13 238:7 243:13 246:21 247:12,23 248:11 259:7 281:1 301:9	306:10 308:12 311:11 <b>pointed</b> 9:11 35:16 120:1 174:14,17 242:8 294:18 299:2 307:2 <b>pointing</b> 299:22 <b>points</b> 77:7 174:20 191:17 247:15 <b>poisoning</b> 114:13,19 <b>police</b> 67:5,6 173:1 174:3 <b>policies</b> 7:3 13:6 34:22 38:1 39:10 44:9 61:12 71:12 81:3 83:19 84:23 85:1 92:18 94:19 94:22 96:18,21 97:11 98:7,10,14 99:5 105:18,19,25 106:4,9,17 109:15 111:21,23 112:1,5 119:20 125:13 138:22 190:6 218:24 220:19,20 221:13 223:19 237:13 250:17 259:19 271:2 272:14,15,20 273:2,7,12,18,18 273:20 274:2,5,7 274:21 275:8,10 275:12,13,15 276:6,6,10,11,12 276:17 277:1,24 277:24 279:21,24 280:15 281:22 282:1,3,4,13,14,14 284:3 285:15,16 285:24 293:13 294:10 297:14 306:8 308:13 309:9 310:20 311:4 312:1 <b>policy</b> 6:13,24 7:11 7:16,18,19 8:4 11:1 14:6 33:3,20	33:25 35:19,20 36:25 39:12,16 46:4 52:21 53:2 54:17 62:3,14 63:2 66:24 79:17,20 80:25 82:4,4,5 85:2,10 95:9 96:12 111:16 113:21 114:3,11,12 116:11 118:5 119:24 123:3 127:2,2 131:5,16 134:15,17 135:1,9 135:15 143:4 158:5 177:13,13 179:5 182:21,24 184:5 189:9 191:17 209:23 223:18 234:6 237:17 245:4 249:2 255:20,20 257:25 259:23,24 264:15 269:2,2 272:4,24 274:20 275:16 276:7,16 276:19,22,24 277:21 278:20,21 278:23,24 280:12 280:12 281:8,12 285:19 293:7 294:1 297:21 298:17 299:15 303:16,20 309:22 312:6,9 313:5 <b>policymaker</b> 238:22 239:2 <b>policymakers</b> 7:11 11:13 13:9 44:25 55:2 116:16 236:4 316:25 <b>policymaking</b> 317:2 <b>political</b> 38:11 59:14 <b>politics</b> 33:22 <b>Polls</b> 41:19 <b>Poneman</b> 230:14 <b>pool</b> 180:20 <b>poor</b> 96:9 183:19	245:20,21 <b>pop</b> 313:10,14 <b>popped</b> 74:12 <b>popular</b> 16:1,4,12 17:1,14,16,17,21 17:25 18:16 19:3 142:9 189:19 192:9,13 194:5,8 250:14 252:7,8 257:3 259:4 266:16 269:21 <b>popularity</b> 193:22 <b>popularized</b> 115:10 <b>populate</b> 153:10 <b>populated</b> 148:11 <b>populating</b> 154:2 <b>population</b> 41:18 49:14,20 51:1 107:24 165:13,22 166:12 168:9,10 182:2 287:18 288:3,10,24,25 289:2 <b>populations</b> 134:1 <b>populus</b> 54:25 <b>popups</b> 77:8,11 <b>port</b> 251:25 253:15 256:14 257:6 <b>portal</b> 279:25 <b>portfolio</b> 190:19 <b>portion</b> 64:6 98:22 <b>ports</b> 254:21,22 258:12 <b>pose</b> 227:11 <b>position</b> 64:25 307:21 309:6 <b>positioned</b> 307:25 <b>positioning</b> 184:2 <b>positions</b> 65:3 <b>positive</b> 48:18 93:3 132:7 198:24 216:23 218:25 219:19 241:22 248:13 <b>positively</b> 217:22 221:16 <b>possibilities</b> 143:15	<b>possibility</b> 50:3 107:20 143:16,23 144:5,20 145:5 <b>possible</b> 8:20 69:9 70:3 75:14 98:23 101:2 107:16 137:3 145:17 262:19 288:3,14 298:24 300:12 <b>possibly</b> 49:2 184:8 214:21 <b>post</b> 5:24 56:4 57:15 246:22 <b>post-doc</b> 272:1,6 <b>Post-Gazette</b> 144:8 <b>postal</b> 103:7 <b>potential</b> 16:16 18:25 55:21 95:20 103:19,21 107:25 110:3 160:14 161:14 180:20 182:21 194:12 211:11,25 212:3,4 239:10,14 250:17 251:15 295:21,21 300:1 311:14 <b>potentiality</b> 300:23 <b>potentially</b> 17:8 18:7 28:5 96:23 97:7 98:12 121:1 134:2 155:9 168:20 194:18 196:25 212:8 215:13 239:5 250:15 253:14 265:23 282:9 290:15 292:16 295:18 307:12 310:2,12 <b>power</b> 43:4,6 117:18 117:23,25 151:3 203:15 205:8 207:8 311:10 <b>powerful</b> 36:6 174:4 199:23 <b>powerlessness</b> 219:15
--	---	---	--	--

<b>practical</b> 13:9 243:5 244:7 294:6	79:10,14 167:11 167:18,24 288:12 288:14,20 289:10 289:25	<b>premiums</b> 168:23	303:16,24 312:15	258:25 269:17 297:1
<b>practice</b> 9:10 39:9 60:17 73:8 85:9,11 86:17,21,23 131:16 189:10 197:16 236:4 279:4,5,5	<b>predictability</b> 156:23	<b>prepared</b> 193:1 198:15 308:9	<b>presenting</b> 14:18 31:16 89:9 100:10 188:8 200:17 210:23 222:5 250:10 299:25 310:10	<b>previously</b> 106:15 108:4 109:18 263:3
<b>practiced</b> 243:10	<b>predictable</b> 49:7 269:8	<b>preparedness</b> 197:4	<b>preserve</b> 76:11	<b>price</b> 50:5 159:9 183:19,24 200:9 223:18 266:21
<b>practices</b> 5:13 9:4 11:23 12:22 16:14 18:10 20:22,22 26:22 33:16 36:21 36:22 37:17 40:12 40:20 50:12 56:17 81:2,7,10,22 83:9 83:9,19,25 84:22 87:19,20,21,23 88:1,11,22 111:19 112:2 133:3 196:17 233:22 272:16 274:4,11 274:24 275:9 276:21,23 278:10 278:13 279:23 280:24,24 281:17 282:12 283:4 304:25 306:2 310:8	<b>predictably</b> 49:6	<b>prescriptions</b> 299:15	<b>president</b> 42:12 222:15	<b>prices</b> 58:16 59:10 151:24 152:7 160:11 163:13,20
<b>practitioner</b> 60:2	<b>predicted</b> 93:12,23 95:6,9,25 96:11,12 96:13	<b>presence</b> 13:12 18:21 19:8 95:8 142:19 268:24 269:13 270:3	<b>press</b> 142:9 252:25 253:1,16,17 254:14	<b>pricing</b> 160:17 162:7 183:14 288:15
<b>practitioners</b> 121:6	<b>predicting</b> 278:6 283:3	<b>present</b> 5:20 14:20 14:21 15:12 35:21 41:11 82:14 86:15 106:11 108:12 136:12 210:17 216:9 222:10 258:22 292:11	<b>pressed</b> 253:19 254:16	<b>primarily</b> 186:14
<b>pragmatism</b> 34:13 34:15,17,21 37:23 53:4	<b>prediction</b> 153:19 153:20 154:8,16 156:11,18 157:4 167:14 168:6,16	<b>presentation</b> 26:6 32:10 68:19 100:6 136:16,19,22 147:20 159:16 172:11 189:16 212:5 239:25 249:9 285:12 294:19 300:10	<b>pressure</b> 185:25	<b>primary</b> 311:3
<b>pragmatists</b> 33:3,9 33:11,14,23 34:11 34:13 35:6	<b>predictions</b> 154:19 168:4,5	<b>presentations</b> 5:8 7:1 11:17 52:6 57:2 68:11 113:17 114:15 130:24 134:5 136:13 171:8,15 234:1,8 303:18 307:22 312:19	<b>presumably</b> 165:16	<b>primitives</b> 157:4
<b>praising</b> 51:19	<b>predictive</b> 43:11	<b>presented</b> 37:2 46:25 83:14 106:7 134:12 233:14 234:9,18 243:6 297:7,16 298:9 304:16 310:15	<b>pretty</b> 67:3 69:2 73:15 77:10 78:6 78:15,17 79:15 94:18 127:14 140:7 148:18 149:1,9 152:12 154:4,5 155:4 157:25 161:18,19 167:16,18 174:10 175:23 185:7 193:14 213:25 251:2,12 254:3,20 256:13 257:3,3 260:23 270:11 291:24	<b>Princeton</b> 16:23 20:2,5 24:5 27:13 45:5 250:7
<b>pre-held</b> 115:11	<b>predictor</b> 78:16 93:21	<b>presentations</b> 5:8 7:1 11:17 52:6 57:2 68:11 113:17 114:15 130:24 134:5 136:13 171:8,15 234:1,8 303:18 307:22 312:19	<b>prevent</b> 61:11 66:4 271:5	<b>principle</b> 7:17 213:13 294:23
<b>precise</b> 152:3 154:19 201:1	<b>predictors</b> 99:3	<b>presented</b> 37:2 46:25 83:14 106:7 134:12 233:14 234:9,18 243:6 297:7,16 298:9 304:16 310:15	<b>preventative</b> 161:21 218:15	<b>principles</b> 121:21 131:15 132:15
<b>precision</b> 152:11 156:23	<b>predicts</b> 95:24	<b>presented</b> 37:2 46:25 83:14 106:7 134:12 233:14 234:9,18 243:6 297:7,16 298:9 304:16 310:15	<b>prevented</b> 75:1 304:13	<b>printed</b> 90:21
<b>precursor</b> 255:1	<b>predominant</b> 205:15	<b>presenters</b> 5:7 51:25 68:13 104:13 110:21 135:16	<b>preventing</b> 66:5 300:24	<b>prints</b> 5:23
<b>predicate</b> 182:25	<b>predominantly</b> 83:1 87:4 141:12		<b>previous</b> 79:15 94:6 95:5 96:2 104:13 106:3,3 110:6 146:13 199:9 201:13 212:5 228:16 229:6 237:8 238:10	<b>prior</b> 25:6 89:17 91:22
<b>predict</b> 55:17 56:8 75:4 77:22 78:3	<b>pregnancy-related</b> 148:25			<b>priorities</b> 11:1
	<b>preliminary</b> 124:15			<b>privacy</b> 2:10,11,14 4:23 5:9,13,21 6:17 7:2,5,15,21 8:1,14 11:14,19,20 12:1,18 13:17,18 14:2,9,10 15:12,15 15:18,20 16:7,10 16:22 17:10 19:13 19:23 20:6,21 22:24 25:25 26:7 26:19 29:10,11 30:3,4,10,23 32:14 32:22 33:3,6,8,11 33:13,21,22,23 34:7,22 35:6,17,19 35:20 36:4,6,7,18 36:19,25 37:13,19 38:1,11,24,24 39:4

39:10,14,16 40:3,6 42:1,2,6 44:9 46:4 52:19,21 53:1,4,12 55:14,21 60:6,11 60:24 63:13,16 65:8 68:2,6,9,24 70:22 71:12 75:24 80:13,17,25 81:15 81:16,21,24 82:1,7 82:16 83:1,19 84:23,24 85:16,23 86:4 87:25 88:6 89:1 90:8 92:14,18 92:20 95:8,15,19 95:24 96:1,5,11,12 96:12 97:3,11,20 98:18 100:10,14 100:22 101:8 102:14,16,20 103:22 104:2,3,5 104:10 105:18,19 105:25 106:4,8,9 106:16 107:8 110:25 111:5,21 111:23 113:3,7 114:1,17,18 117:10 119:16,24 123:3 125:13,19 125:21 127:4 130:6 131:4,5,10 131:13,19 132:2 136:19 138:3,5,22 142:14 151:3 171:20 182:24 188:2,6 200:5,9 204:15 209:14 210:8,12,17,22,25 211:10,11,14 212:5,10,15 213:20 214:4,11 214:20,24 215:22 218:12,20,24 219:22 220:5,8,10 220:19,20 221:17 224:8,23 225:2,6 226:18 228:21,24 228:25 229:10,16	229:21 231:7,10 234:19 235:7,11 235:18,22 236:11 236:19,21 237:13 239:3,9,12,16,17 240:15 241:8,11 241:15 242:5 243:14,18,22 244:9,20 245:10 245:13 250:5 251:15 259:19,23 264:12 265:17 272:4,14,15,20,24 273:2,7,17,19 274:2,7,9,21 275:2 275:4,12 276:9,16 277:24,24 278:23 280:1 281:8,10,22 282:1 283:3,7,14 284:3 285:1,3,6,7 285:15,16,22 286:3,6 287:15 289:20 290:9 291:1,6 293:7,13 293:15,21 294:4 295:11,16,19 296:7,9 297:2,4,6 297:13,17,17,20 298:5 299:12 304:12,15,16,20 305:19,24 308:13 309:18 310:20 311:4,25 312:16 312:20 313:5,5 315:23 317:1 <b>privacy-enhancing</b> 242:21 <b>privacy-friendly</b> 243:5 <b>privacy-preserving</b> 244:2 <b>PrivacyCon</b> 1:4 3:4 4:17,22 5:10,18 6:23 11:10 14:5 54:15 112:20 115:4 116:14 130:14 134:6	135:6 136:5 318:3 <b>private</b> 38:5,15 55:21 68:24 92:7 103:24,25 135:18 221:2 226:10 228:10,11 242:12 242:17,20 254:24 <b>proactive</b> 118:6 146:4 <b>proactively</b> 118:10 146:3 172:18 173:16 <b>probably</b> 25:6 38:25 53:19 71:16 72:2,4 72:18 124:16 126:9 130:19 134:21 143:4 148:5 160:10 177:10 178:9 208:21 211:25 217:19 222:14 283:1 284:9 310:1 <b>problem</b> 10:11 20:7 20:7 32:16 34:9 37:9 63:3 70:10 71:11 72:15,24 80:7 114:3,12,12 137:9 145:19,19 150:7 160:7 161:18 173:19 174:23,24,25 175:13 184:3 199:19,20 237:6 237:23 243:18 250:20 252:2 268:10,17 298:16 298:22 299:11,17 306:10,21 311:7 311:24 312:1,2,7 <b>problematic</b> 35:7 107:3 122:3 173:17 181:10 <b>problems</b> 9:11,24 34:19 40:6 58:25 62:16 75:11 107:7 122:22 146:10 161:7 162:20	237:8 251:16 299:13 300:23 <b>proceedings</b> 67:22 187:1 249:16 <b>process</b> 9:9 10:5 56:24 59:14 70:16 72:2 88:4 152:21 154:2 201:12 202:3 204:4,5 205:19 206:25 207:20 219:12 225:10 232:22 281:14,18 <b>processes</b> 63:20 <b>processing</b> 85:6 132:20 274:6 278:1 280:6 281:24 <b>produce</b> 134:9 155:10 164:5,24 175:22 <b>produced</b> 167:2 230:15 <b>produces</b> 8:18 <b>product</b> 108:7 117:3 117:5 120:24 202:24,25 203:7 205:21 279:17 <b>products</b> 5:25 34:23 40:8,10 181:17 201:24 203:9 205:23 <b>profession</b> 63:16 <b>professional</b> 101:22 <b>professor</b> 2:6 35:15 41:2 260:19 282:22 <b>profile</b> 25:21 59:8 118:24 119:2 174:19 289:8 <b>profiles</b> 163:18 174:21 176:22 178:2 290:7,8 <b>profiling</b> 50:23 286:17 <b>profit</b> 204:18 205:1 205:2 206:8,10,16	206:19,21 <b>profit-generating</b> 55:23 <b>profit-maximizing</b> 202:23 203:5 <b>profitable</b> 43:9 <b>profits</b> 208:16 <b>program</b> 7:13 11:15 44:19 139:2 172:9 188:18 189:25 193:22,22 195:15 195:18 201:18 246:19 272:6 <b>programing</b> 293:11 <b>programmed</b> 143:18 <b>programmers</b> 143:17 250:23 <b>programs</b> 135:2 171:18 188:21 189:18 190:17,22 191:22 192:19 194:4,5,17 195:24 196:5,20 197:2,14 197:17,25 198:22 234:9 246:15,20 246:24 247:8,13 259:9 <b>progress</b> 13:5 210:5 283:1 <b>project</b> 19:14 69:15 89:12,15,25 159:24 261:12 272:3,4,5,6,7,10 272:13 273:25 274:14 281:21,25 309:20 <b>projects</b> 130:24 <b>proliferation</b> 52:7 <b>prominent</b> 19:1 <b>promise</b> 212:20 262:18 272:15 <b>promising</b> 244:6,7 312:22 <b>promoting</b> 123:25 124:1 <b>prompt</b> 72:13 74:20
--	---	---	---	--

78:1 <b>prompted</b> 55:18 <b>prompts</b> 80:1,1,4 112:14 <b>prone</b> 65:5 <b>proof</b> 185:14 217:25 <b>proofed</b> 140:3 <b>proofread</b> 318:19 <b>proper</b> 246:1,10 308:8 <b>properly</b> 132:14 <b>properties</b> 21:11 152:2 156:1,22 <b>property</b> 214:6,15 217:17 224:1,22 <b>proportion</b> 41:18 46:1 216:16 226:20 227:15 <b>proposals</b> 14:14,15 64:1,2 273:17 <b>proposed</b> 234:12 273:24 <b>proposition</b> 44:15 <b>propositions</b> 45:21 45:22 <b>proprietary</b> 225:13 <b>ProPublica</b> 21:25 23:11 <b>pros</b> 198:19 <b>protect</b> 5:12 8:6,14 23:8 50:5 61:13 108:20 113:3,8 118:6 222:18 263:23 264:13 270:23 <b>protected</b> 12:6 30:7 75:10 112:15 163:25 164:10,11 164:21 166:8 173:12 <b>protecting</b> 26:1 220:9 265:23 307:7 <b>protection</b> 6:20 7:20 11:8 14:9 68:6,7 101:25 102:9 108:10 117:9	118:9,12 209:15 210:17 231:7 240:16 243:21 315:23 <b>protections</b> 9:18 26:20 102:10 126:18 210:25 212:16 245:14 264:13 265:11 <b>protective</b> 50:17,18 <b>protocols</b> 247:21 251:1,3,18 257:18 258:12 260:7 <b>proud</b> 31:17,19 <b>prove</b> 208:24 219:22 <b>proved</b> 155:21 <b>provide</b> 7:8 8:5 24:3 30:3,9 45:19 47:19 110:20 120:6 130:4 138:10 140:10 154:18 189:8 190:13 248:17 274:10,19 280:22 298:4 308:15 <b>provided</b> 3:19 9:18 22:4 82:17,18 138:3 167:6 197:17 260:3 274:23 297:19 <b>provider</b> 19:11 22:4 22:7 <b>providers</b> 262:12 272:16,18,22 <b>provides</b> 6:21 20:14 20:14 154:10 156:17,21 157:3 163:13 223:22 247:16 275:19 279:22 <b>providing</b> 19:4 104:3 112:17,22 133:22 138:16,17 165:10 170:7 274:23 313:3 <b>provision</b> 245:15 <b>provocative</b> 7:1	243:24 <b>proximity</b> 180:13,15 180:17 <b>proxy</b> 24:25 180:24 <b>PSA</b> 99:11,19 <b>psychological</b> 267:1 <b>public</b> 4:3,11 10:9 29:23 33:3 38:9 44:24 51:15,18 55:18 101:5 102:13 104:1,6 113:21,25 114:3 114:11,12 118:5 119:16 127:19 134:15 135:1,9,18 151:12 184:5 189:15 190:9,16 196:19 197:17 200:4 225:12 226:3,10 271:8 274:20 276:7 281:20 294:1 <b>public's</b> 44:4 59:12 102:19 103:23 <b>publicized</b> 221:22 <b>publicly</b> 127:19 191:14 <b>publish</b> 240:18 299:9,10 <b>publishable</b> 35:10 35:12 <b>published</b> 31:22 35:9 <b>publisher's</b> 202:5 <b>publishers</b> 23:18 201:21 <b>pull</b> 130:18 <b>pulled</b> 218:16,17 <b>pulling</b> 27:21 <b>punch</b> 216:10 <b>punched</b> 39:22 <b>punctuation</b> 318:21 <b>purchase</b> 4:4 104:25 106:12 120:16 128:12 203:15 204:2 205:8 <b>purchases</b> 46:9	47:10 <b>purchasing</b> 108:7 144:24 <b>purely</b> 287:4 <b>purpose</b> 86:25 111:14 151:20 172:14 193:18 224:16,20 287:5 <b>purposes</b> 87:2 106:2 109:22,24 150:4 150:11 168:22 286:15,16,17 287:4 <b>purview</b> 133:18 <b>push</b> 43:8 122:10 214:17 <b>put</b> 14:13 42:19 49:5 66:6 99:25 117:19 138:18 207:3 303:9 307:14 <b>puts</b> 156:19 268:19 273:11 <b>putting</b> 13:20 31:15 118:5 119:11 126:13 179:25 235:1 310:9 <b>puzzle</b> 186:13	73:6 81:20 90:1,20 92:13 96:23 109:23 120:21 125:17 142:15,21 172:17 177:4,7 184:1 191:5 192:3 193:3,7 194:24 200:24 201:7 222:24 223:4 229:23 230:13 231:4 235:23 241:4 242:6 244:12 247:3 261:2,9 262:13 263:7 267:14,19 267:20 268:1 275:17,18 284:21 292:2 300:3 302:5 303:15,23 307:9 315:3,4 <b>questionable</b> 140:5 184:12 237:8 <b>questioning</b> 55:3 <b>questionnaires</b> 74:14 <b>questions</b> 13:9 15:7 16:11 34:3,20,20 35:1,4,5 37:3,6 46:6 47:12 74:17 80:21,24 82:21 85:1,7 90:4,7 92:8 104:8 110:24 113:14 114:8 116:19 131:12 132:15,23 135:9 141:23 142:12,18 144:7 147:8 150:14,15 186:16 209:9 222:18 235:4 275:24 279:2,7 289:10,15 289:17 290:12 296:6,8,21 301:7 303:10 <b>quick</b> 26:23 67:18 98:15 176:8 192:19
<b>Q</b>				
<b>QUADE</b> 318:15 <b>qualitative</b> 69:21 90:3 91:5,7,9,18 91:23 133:1 240:6 <b>quality</b> 117:3 130:24 191:8 277:6 <b>Quantcast</b> 16:21 <b>quantification</b> 156:17 <b>quantifying</b> 275:11 <b>quantitative</b> 91:5,13 <b>Quarterly</b> 38:10 <b>querying</b> 76:13 <b>question</b> 11:21 34:5 34:6 53:17 54:20 55:25 62:2,3,21 65:9,18 69:11 72:5				

<b>quickly</b> 41:5 97:14 103:5 119:19 133:19 139:5 148:22 152:20 201:19 284:14 293:25 301:6	<b>ramifications</b> 310:5 <b>Ramirez</b> 2:4 5:11,14 5:16 14:4 113:5 130:16 <b>rampant</b> 112:3 <b>ran</b> 16:24 120:10 167:4 290:17,18 <b>RAND</b> 222:4 233:5 233:7 <b>random</b> 153:13 178:22 213:25 254:20 267:10 <b>randomly</b> 74:15,18 139:10 153:11,13 <b>range</b> 191:10 <b>rank</b> 127:10 165:2 192:10 <b>Rao</b> 80:12,15 285:13 <b>rapid</b> 6:16 <b>rarely</b> 247:1 <b>rate</b> 57:13 145:11 167:14 168:5,6 169:14 226:17,24 227:15,19 228:1,3 228:20 229:4,7,10 234:18,23 248:9 <b>rates</b> 169:15,25 177:22 231:18 234:22 <b>ratio</b> 141:4 <b>rational</b> 32:15,18,24 33:2 42:16 246:8 302:23 <b>rationale</b> 47:18 50:20 <b>rationally</b> 51:8 304:14 <b>ratios</b> 248:1 <b>raw</b> 66:24 <b>RCT</b> 38:17 <b>re-admission</b> 167:14 <b>re-admitted</b> 167:20 167:24 <b>re-examining</b> 89:13 <b>re-identify</b> 101:3,6 <b>reach</b> 153:21 266:19 277:14 289:15	<b>react</b> 217:11 <b>reacting</b> 63:8 <b>reaction</b> 58:12 217:16 <b>read</b> 29:3 34:22 36:24 39:1 40:21 42:5 53:1 64:6 80:25 81:4 84:25 88:3 97:11 98:13 99:8 106:16 107:2 107:5,6 115:8,8 119:24 123:2 170:12 253:3 264:3 265:5,6,7,14 265:18 266:2,8 268:5 269:3,4 272:10 278:18,19 282:13 284:3 285:16 294:10 <b>readability</b> 99:5 <b>readable</b> 98:7,10 <b>readers</b> 23:15 54:2 <b>reading</b> 90:21 94:11 96:18,21 114:16 128:7 278:23 <b>readings</b> 255:13,25 255:25 <b>ready</b> 135:13 <b>real</b> 24:9 25:23 46:5 49:15 58:25 73:9 74:10 145:17 165:21 166:23 169:3 170:8,8 174:18,23 175:1,9 175:11,12,15,22 176:10,17 177:2 263:18 290:6 299:1 311:24 312:10 317:1 <b>real-life</b> 210:22 <b>real-time</b> 75:7 <b>real-world</b> 177:20 178:21,25 <b>realistic</b> 155:8 175:8 302:25 304:1 <b>reality</b> 32:6,6 72:9 112:4 114:10	154:11 272:19 <b>realization</b> 48:3 <b>realize</b> 73:25 100:18 101:14 102:3 105:3 176:4 182:3 204:6 215:24 284:14 304:19 308:15 <b>realized</b> 103:5 <b>realizing</b> 284:5 <b>really</b> 14:14,15 20:24 21:23 22:16 24:7 30:1,24 34:20 35:7 40:2,2 41:12 41:17 42:24 43:25 44:9 50:11 51:3,4 52:18 53:17,20 54:16 56:7 58:13 59:5,20 61:17 62:7 63:21 65:12,21,23 67:7,8 70:25 73:4 73:7 75:15 77:1,6 77:12 78:3 79:2,4 89:15 92:1 94:13 95:1,14 96:24 97:13,14 99:3,9,11 99:14 107:3,4,6 108:8 110:4,7 115:7,16 120:11 121:18,21 122:3 123:4 127:23 130:12,15,20,20 132:14 136:5,11 146:17,21 149:2 150:12,23 162:20 162:22 165:11,12 165:21,22 166:11 168:2,15,15,20,24 170:8,21,22 173:3 173:25 174:4,15 174:22 178:5 179:10 180:2 183:18 184:20 193:16,17 196:22 197:13 198:9,11 209:6,9 212:9 216:21 217:9	218:16 219:8,22 221:14 223:16 226:22 228:9 229:11,12,16,17 229:20 233:12,12 233:15,17,21 235:16 237:4,9,16 238:3,4 239:2,5 240:13,13 242:21 243:17 244:20,21 246:15 248:12 249:13 250:14 254:21 259:3 265:10,16 266:11 270:17 272:22 273:9,11,21,25 274:12,25 275:20 276:3 278:14 279:14,22 280:5 281:25 282:6,16 285:25 294:11,11 295:8,13 298:9,15 299:1,16 301:6 303:1 306:12,14 306:17 307:9 308:25 311:8,9,12 311:18 312:6 314:9,17 315:18 <b>realtime</b> 201:16,16 <b>reason</b> 35:23 36:1 79:19 181:15 211:6,23 212:11 213:24 214:16 215:10 220:1 241:16 243:13,22 264:23 267:25 268:1,4 269:15 276:16 284:4 287:9,14,22 311:3 <b>reasonable</b> 39:17 55:6 72:20 89:9,13 123:12 152:11 193:5 196:11 224:16 240:2 261:2 <b>reasonableness</b> 89:21
<b>R</b>				
<b>R</b> 3:1 318:1,1,1,1,17 318:17,17,17 <b>race</b> 49:21,23 162:6 162:13,15 164:12 212:14 214:23 241:14 242:2 244:8 309:19 <b>races</b> 182:6 <b>racial</b> 91:11,19 181:5 <b>radical</b> 65:3 <b>radically</b> 6:5 <b>radio</b> 253:1,8,18,21 253:22 <b>raided</b> 270:3 <b>raise</b> 95:4 179:24 <b>raised</b> 106:22 <b>raises</b> 191:4 193:3 <b>raising</b> 247:4				

<b>reasonably</b> 263:10 263:10 270:21	<b>record</b> 24:25 220:5	242:5	140:18 147:4	157:1 166:9
<b>reasons</b> 76:10 181:11	<b>recorded</b> 4:12 226:9 228:7	<b>region</b> 205:13,16,20 206:1,4,9,12,20,23 207:6,11	186:16 222:11 224:2 246:21 297:5	<b>remains</b> 133:9
<b>reassure</b> 221:23	<b>recording</b> 229:2,3	<b>regions</b> 206:8	<b>relates</b> 200:18 250:4 297:3 298:5	<b>remarks</b> 2:3 5:10 130:4,13 170:10 208:18 314:3
<b>reassured</b> 219:9	<b>records</b> 167:8	<b>register</b> 292:12	<b>relating</b> 127:12 224:5	<b>remedy</b> 40:6
<b>reassuring</b> 241:16 242:2	<b>recreation</b> 105:9	<b>registration</b> 3:15	<b>relations</b> 59:13	<b>remediating</b> 274:22
<b>recall</b> 152:12	<b>recreational</b> 109:22 109:24	<b>regression</b> 93:8 94:16 95:22 193:19	<b>relationship</b> 43:9 48:19,22 59:6 180:4 182:9 216:1 221:17	<b>remember</b> 128:17 152:22 180:13 216:16 268:11
<b>recap</b> 234:3 293:25	<b>recruited</b> 84:19 276:8	<b>regression-based</b> 278:9	<b>relationships</b> 93:1 126:18 134:14 307:16	<b>remind</b> 143:11
<b>recaps</b> 234:16	<b>recruiting</b> 39:21	<b>regressions</b> 156:7	<b>relative</b> 232:16	<b>remotely</b> 108:2
<b>receive</b> 47:4 194:8	<b>red</b> 206:20 207:11 208:1	<b>regularly</b> 267:3	<b>relatively</b> 15:25 126:25 276:21 278:23 312:8	<b>remove</b> 22:22 40:14 removed 9:9 22:15 23:16 196:24
<b>received</b> 3:14 204:18	<b>redisclosure</b> 234:21	<b>regulate</b> 214:20 239:3 245:10	<b>release</b> 5:4 41:24 125:25 271:15 279:25 281:20	<b>removed</b> 9:9 22:15 23:16 196:24
<b>receives</b> 202:11 203:5,20,24	<b>redress</b> 56:24 230:11	<b>regulated</b> 68:24 69:6 71:2 222:23	<b>released</b> 12:1 30:6 125:20	<b>rent</b> 209:21
<b>receiving</b> 171:11 194:6 197:5 198:16	<b>reduce</b> 88:25 97:3 213:13 234:11 280:18 285:2 302:24 314:25	<b>regulating</b> 214:6,24 230:12 298:23 311:10	<b>releasing</b> 21:22 61:13 212:1	<b>repairing</b> 230:7
<b>reception</b> 219:18	<b>reduced</b> 10:6	<b>regulation</b> 55:20 127:23,24 210:22 212:13 213:20 214:4,11 221:17 227:2 245:4 308:17 311:16,17	<b>relevant</b> 7:10 278:7 280:23 281:17 282:16 293:16	<b>repeat</b> 65:17 116:15 231:14,21 232:1,5 232:9 262:13
<b>recess</b> 67:21 129:3 186:25 249:15	<b>reduction</b> 88:2,13 216:14 312:12	<b>regulators</b> 26:8 89:22 117:4,9,15 273:1 282:8 297:15	<b>reliable</b> 19:14 32:19	<b>repeated</b> 16:7 repeatedly 41:19 184:13
<b>recognition</b> 7:24 54:4 56:6 57:21 101:1 284:19	<b>refer</b> 237:23	<b>regulations</b> 216:11	<b>reliably</b> 270:11 277:2	<b>replace</b> 306:18
<b>recognizable</b> 263:12	<b>reference</b> 21:4	<b>regulatory</b> 57:24 101:22 118:9 131:9 184:19 243:25 272:25 311:5	<b>reliance</b> 278:9	<b>replaced</b> 72:4
<b>recognize</b> 20:13 42:10 50:3 60:10	<b>referred</b> 201:3	<b>regulators</b> 26:8 89:22 117:4,9,15 273:1 282:8 297:15	<b>reliant</b> 278:9	<b>replicate</b> 37:14 40:4
<b>Recognizing</b> 10:8	<b>referring</b> 237:7	<b>regulations</b> 216:11	<b>rely</b> 97:10 123:19 175:3 201:8 202:1 203:1 244:14 254:21 264:12 295:17	<b>repliers</b> 181:23
<b>recommend</b> 290:14	<b>reflected</b> 52:8 311:25	<b>regulators</b> 26:8 89:22 117:4,9,15 273:1 282:8 297:15	<b>relying</b> 111:22 239:4	<b>repo</b> 31:6
<b>recommendation</b> 94:14 96:5 126:10 291:10	<b>reflecting</b> 41:23	<b>regulators</b> 26:8 89:22 117:4,9,15 273:1 282:8 297:15	<b>remain</b> 3:18,23 56:5 92:14 192:15	<b>report</b> 8:16,20 58:6 125:20 133:21,23 134:3 164:6 180:18 248:7 274:16
<b>recommendations</b> 71:8 94:13 150:5,6 151:24 152:6 163:14 237:17 290:21 291:5,9,13 291:18,21,24	<b>reflective</b> 41:17	<b>regulatory</b> 57:24 101:22 118:9 131:9 184:19 243:25 272:25 311:5	<b>remaining</b> 151:10	<b>reported</b> 194:4 196:10 226:8
<b>recommended</b> 112:15 300:5	<b>reflects</b> 42:16	<b>regulatory</b> 57:24 101:22 118:9 131:9 184:19 243:25 272:25 311:5		<b>reporting</b> 133:17 227:4
<b>recommender</b> 79:24	<b>reform</b> 107:4	<b>rehab</b> 141:15,17 147:7		<b>reports</b> 7:23 8:5 10:16 62:24 93:14 114:16 133:15 139:17 164:22 189:21 194:6 196:2,6 197:6,23 198:17 232:24 247:1 248:1,4,6
<b>recommending</b> 112:11,13,16	<b>refusing</b> 220:9	<b>Reidenberg</b> 275:2		<b>represent</b> 226:20,22 228:23,25 230:8,9
<b>recommends</b> 94:15 133:23 134:3	<b>regard</b> 79:5 119:16 127:22 227:7 228:24	<b>reinforce</b> 8:25		
<b>reconstruct</b> 156:3	<b>regarding</b> 17:6 41:13 131:17 237:10 256:23 258:14 260:6	<b>rejecting</b> 48:20,24		
	<b>regardless</b> 49:20 118:19 120:3 312:6	<b>relate</b> 59:20 70:20 215:20 236:4		
	<b>regards</b> 87:3	<b>related</b> 45:2 89:22 90:5,7,7 92:6,18 111:14 127:8		
	<b>regime</b> 215:22			
	<b>regimes</b> 241:15			

232:12	99:19 100:14	41:17 48:2,15,15	<b>restaurant</b> 117:5	<b>revealed</b> 206:4,11
<b>representations</b>	102:18 103:1,10	49:19 53:4,5	<b>restore</b> 219:17	206:17 207:13
116:24	105:1,18 106:13	<b>resigned</b> 48:23,25	<b>restrict</b> 217:20	<b>revealing</b> 205:21
<b>representative</b>	107:14 109:21	49:4,7,9,14,17,24	<b>restricted</b> 234:21	206:24 207:10,11
165:13 220:23	113:7,9 120:23	50:13,13 51:1 55:6	<b>restricting</b> 214:14	<b>reveals</b> 270:14
<b>representatives</b>	128:7 130:13	55:15 57:4,10 58:9	<b>restriction</b> 216:18	<b>revenue</b> 232:13,15
208:22	134:10,11,12,16	61:3 115:21 116:1	<b>restrooms</b> 4:9	233:2 263:14
<b>represented</b> 199:12	135:8,10,14	118:18 281:4	<b>result</b> 8:21 13:4 17:9	<b>reverse</b> 261:16
279:23,24	136:13 141:25	<b>resist</b> 56:17	34:18 43:7 49:17	262:21
<b>republished</b> 39:1	142:5 146:15	<b>resisting</b> 47:25	77:7 93:24 94:1	<b>reverses</b> 169:23
<b>reputable</b> 263:10	147:10 159:16	<b>resolve</b> 234:11	96:7 114:14 121:9	<b>reversible</b> 71:21
<b>reputation</b> 248:14	160:2 163:1	<b>resource</b> 80:9	146:13 158:4	<b>review</b> 5:5 133:24
263:13 299:4	172:19 175:14	<b>resources</b> 112:15	171:11 185:4	215:3 236:11
<b>request</b> 70:4 72:14	176:13,19 185:1,2	292:9,9,11,13,16	213:10 215:16	<b>reviewers</b> 240:23
72:20,22 77:4	189:10 195:19	293:3,5,6,10,16	269:17 270:12	<b>reviewing</b> 220:20
118:23 144:4	199:18 200:13	<b>respect</b> 39:6 91:2	271:1 273:6 288:1	<b>reviews</b> 38:9,12
<b>requested</b> 72:7,25	209:9 217:20,21	113:10 117:9	297:9	52:20 180:1,2
73:12,17,19 77:11	221:21 228:16	175:24 190:4	<b>resulted</b> 75:6 99:13	<b>revised</b> 52:10
111:18	235:17 236:5,12	239:25	<b>resulting</b> 43:11	<b>revision</b> 283:6
<b>requesting</b> 69:10	241:6,10,17,19	<b>respectable</b> 263:10	98:19	<b>revisit</b> 286:4 291:11
70:3 71:5 73:22	242:11 245:12	<b>respected</b> 104:9	<b>results</b> 16:10 41:10	291:14
74:22,24 75:17	275:1 280:6 288:2	<b>respond</b> 113:16	86:5 87:16 91:14	<b>rhetoric</b> 32:3,11
78:17	288:23 297:3,12	192:5,11 233:9	100:16 102:23	<b>rhetorical</b> 60:9
<b>requests</b> 26:16 69:5	297:20 301:10,11	235:14 309:17	103:8 105:9 121:5	<b>rich</b> 183:20 264:23
70:7 75:9 76:9	303:17 312:16	<b>responded</b> 23:13	121:7 127:14	264:25 279:22
77:3,9,17,18 78:10	313:17 314:18,20	<b>respondents</b> 103:12	147:7 156:13	<b>richer</b> 7:4
78:21,23 225:16	314:23 315:9,13	103:13,14,19	158:20 171:10	<b>richly</b> 131:6
<b>require</b> 284:11,14	315:21,24 316:4,8	104:15	175:6 197:19	<b>ride</b> 54:8 57:5
<b>requirement</b> 226:4	316:10,11,12,25	<b>responding</b> 67:10	198:4 204:23	<b>right</b> 14:23 20:11,19
<b>requires</b> 3:17,20	317:2	<b>response</b> 21:24,25	208:24 216:9	20:24 23:21,25
9:15 34:13,14	<b>researched</b> 95:17	23:5 58:6 67:15	217:2 220:11	25:8,21 27:20
39:17 70:25 71:5	<b>researcher</b> 25:10	144:7 192:19,21	251:15 252:10	28:21,24 29:2,7,23
132:23 254:7	157:13 209:19	312:2,2	276:1,14 277:5	35:18 36:23 42:11
261:15 286:15	<b>researchers</b> 7:9 9:3	<b>responses</b> 26:16	283:5 312:23	44:3 48:9 51:20,20
<b>requiring</b> 227:2	9:11,19,22 31:16	116:20 124:18	315:19	52:13 53:4,14,16
293:10 308:21	68:10 95:17	233:13	<b>retail</b> 12:8 232:18	53:23 54:8 56:25
<b>research</b> 3:5 4:21	132:25 133:12	<b>responsibilities</b> 92:6	<b>retailers</b> 44:14	61:12,12,18 62:5,8
5:9,21 6:14,15,19	136:12 145:21	<b>responsibility</b>	<b>rethink</b> 7:3 290:25	62:9,13,22 63:4,20
7:1,13,16,17,19	146:9 188:17,19	117:25 142:21,25	291:15 304:21	66:1,6,10,14,19,22
10:19,22,25 11:6	194:3,12,23	143:9 146:6	<b>retrieve</b> 44:14	78:11,19,24 79:13
11:17,25 13:7,8	195:16 237:14	147:12 186:11,16	<b>retrieved</b> 148:15	90:18 93:2 95:12
14:7,13,21 19:14	238:11 247:18,19	<b>responsible</b> 62:9	<b>return</b> 3:15 12:5	97:17 105:2
26:5 31:7 44:13	247:21 248:5	142:16 143:16	<b>returned</b> 73:14	114:12 116:23
45:5 55:12 58:8	316:2,6	259:8,14	<b>returning</b> 23:18	117:7,11,12,14
63:23 82:10,21,24	<b>researching</b> 34:23	<b>responsibly</b> 6:13	<b>reuse</b> 3:15 154:21	118:1 124:14
83:1,3 95:21 96:2	<b>residence</b> 270:16	<b>responsive</b> 116:12	170:17	132:2 149:1,7,8
97:16,21 98:5	<b>resignation</b> 41:13	<b>rest</b> 22:17 96:20	<b>reveal</b> 150:25 152:5	159:4 161:5

170:20 171:20,24 172:12,15,15,24 173:6,10,19,23 177:23,23 179:15 180:21 181:10,18 181:22 182:8,17 183:22 185:6,12 185:23 209:8 229:7 237:22 238:8 239:21 242:12,18 243:11 243:20 244:12,18 245:23,24,25 246:1,5,11,14,20 248:19 249:1 252:2,15,21 257:1 259:17,22 260:10 260:16 266:10 271:8 274:16 275:11,17 290:2 292:7 294:6 295:3 301:21 302:23 304:13 307:10,14 307:18 308:13 309:12,19 312:7 <b>right-hand</b> 148:16 290:15 <b>rights</b> 15:19 37:16 38:19,20 131:13 214:7,15 217:17 <b>rigor</b> 137:4 139:25 <b>rigorous</b> 142:1 146:14 154:17 240:18,23 <b>rises</b> 239:18 <b>rising</b> 230:24 <b>risk</b> 8:22 71:19 107:16 108:2 109:24 114:25 117:13 124:3 223:15,17 227:8 227:12 302:7 311:4 <b>risks</b> 8:10,20 107:8 107:18,19 121:3 127:8,12,14,25 224:10 246:6	299:12 301:4 307:13 <b>risky</b> 299:21 <b>road</b> 66:19 67:2 239:15 <b>robocall</b> 10:10,11 <b>robocalls</b> 9:24 10:18 <b>robust</b> 73:15 135:17 235:22 239:13 276:1 <b>role</b> 9:19 57:7 197:11 201:14 203:10 304:3 <b>roles</b> 272:20 <b>Romanosky</b> 222:4,7 222:10 237:21 244:11 245:18 <b>room</b> 66:13 115:3 128:21,23 133:11 208:23 220:18 256:2,4 286:1 292:14,20 304:2 <b>rooms</b> 4:6,6 128:14 <b>roster</b> 5:6 <b>roughly</b> 18:1 262:21 293:24 <b>round</b> 130:21 314:6 <b>routers</b> 292:19,21 <b>Roxana</b> 145:24 147:21 159:13 184:6 <b>RSS</b> 252:23 <b>rule</b> 94:14 141:6 143:20 <b>rules</b> 35:17 36:22 54:11 60:17 <b>rumors</b> 191:15 <b>run</b> 3:7 24:8,8,10,21 24:24 25:13,16,24 27:24 28:25 29:12 30:22 74:8 139:4,5 157:24 163:6 179:14 188:21 189:24 190:17,22 203:25 204:24 221:16 296:22 <b>running</b> 73:24 75:20	78:16 110:4 140:10 171:14 196:1 247:12,17 265:12 267:8 268:14 269:12 270:12 303:14 <b>runs</b> 24:20 <b>runtime</b> 72:5,13 77:3 112:13 <hr/> <b>S</b> <hr/> <b>S</b> 3:1 <b>S.W</b> 1:10 <b>Sadeh</b> 282:22,24 303:25 309:17 312:18 313:18 <b>safe</b> 95:4,7 265:4 <b>safety</b> 96:19 98:4 124:5 <b>sake</b> 276:14 <b>sale</b> 107:9,10 109:16 <b>SALLY</b> 318:15 <b>Salsburg</b> 4:18,19,20 13:19 136:3 147:19 159:2,13 159:15 171:5 174:6,17 177:4 185:17 186:1,19 <b>sample</b> 102:24 103:6,16 215:2,5 215:17,21 229:13 <b>samples</b> 108:18 <b>Samsung</b> 257:2 <b>sanctions</b> 230:11 <b>sandboxing</b> 264:16 <b>sanity</b> 162:11 <b>SARA</b> 318:24 <b>Sarthak</b> 250:6,9 294:18 297:5 313:20 <b>Sasha</b> 222:4,10 233:25 234:24 <b>Sasha's</b> 239:21 240:7 <b>SaTC</b> 272:5 <b>satisfied</b> 52:22 <b>satisfy</b> 240:23	<b>save</b> 37:9 213:1,1 215:12 <b>savior</b> 43:11 <b>saw</b> 21:22 22:20,21 22:25,25 23:1,6,9 28:14 39:4 44:22 52:6 115:19 239:21 247:10 253:11 254:5 255:6 314:23 315:21,24 316:2 <b>saying</b> 23:7 39:14 42:24 49:4 58:22 58:24 65:19 85:24 159:25 173:25 178:14 179:8 184:15 218:2 229:24 233:1 251:24 276:2 298:14 299:9,10 301:6 302:22 308:3 <b>says</b> 39:16 42:8,12 42:21 45:10 46:7 120:14 178:23 216:19 269:2 <b>scalability</b> 156:23 175:20 <b>scalable</b> 62:21 152:4 175:20 <b>scale</b> 24:18 25:18 85:4 91:25 92:10 92:21 146:24 147:22 148:3 154:11,19 159:7 175:23 184:9 281:9 <b>scaling</b> 155:14,14 <b>scary</b> 59:11 <b>scenario</b> 46:5 47:24 84:5,6 207:21 208:7 302:15 <b>scenarios</b> 46:20 145:14 201:10 205:3,12,13 207:17 209:23 <b>scenes</b> 133:6	<b>Schaub</b> 271:25 272:2 308:11 310:13 313:1 <b>schedule</b> 14:17,20 15:3 <b>scheme</b> 279:14 <b>scholars</b> 143:3 236:14 <b>scholarship</b> 130:12 <b>school</b> 44:21 110:18 169:8,9 171:7,16 234:6 236:14 282:23 <b>schools</b> 44:18 134:20,23 <b>science</b> 68:17 131:2 134:25 139:25 142:1 143:5,6 167:3 171:19 188:13 271:21 282:23 302:3,6,7 302:18 <b>sciences</b> 135:2 <b>scientific</b> 137:4 <b>scientists</b> 38:11 135:7 143:3 <b>scoop</b> 5:23 <b>scour</b> 225:15 <b>scratching</b> 13:3 <b>screen</b> 44:6 52:13 69:8,17 73:24 74:15,18,21 75:19 138:5 <b>screening</b> 34:20 128:20,24 <b>screens</b> 69:18 <b>scripts</b> 30:6 <b>scrolling</b> 314:14 <b>scrutinize</b> 188:20 <b>seal</b> 35:19 <b>seals</b> 39:10 <b>search</b> 164:16 177:16 278:20 <b>searched</b> 252:7 268:3 <b>searches</b> 151:22 <b>searching</b> 178:3
--	---	---	---	--

<b>seats</b> 68:3	239:23 241:11	198:12 200:14	<b>Selenium</b> 24:21	203:9 213:16
<b>second</b> 3:10 22:6	246:13,16,16,18	205:5,22 207:4,19	27:24 29:17	218:19 219:15
36:1 68:8 92:9,20	246:19 247:9,12	211:22 213:25	<b>self</b> 55:14 94:10	226:12 243:14
93:5,17 99:10,10	247:17,18,21,23	218:6,9 221:3,4	174:10	247:18 251:24
112:1 116:4 132:5	248:7,14 250:2,4	224:4 226:13,21	<b>self-determination</b>	256:2 282:17
136:7 137:5	251:1,3,18 254:3,4	228:20 236:2,23	131:11	288:19 301:24
153:15 191:7	254:7 255:19	237:1 242:19,23	<b>self-help</b> 299:3	311:2
222:12 234:17	258:3,15,17,18	242:23,25 243:9	300:20 301:1,3,12	<b>sensing</b> 156:2 292:9
254:2 258:20	259:19,23 260:4	245:8,12,16 253:6	301:17	<b>sensitive</b> 69:6,9 70:2
269:25 302:14	260:10,12 264:12	253:10 256:7	<b>self-regulation</b> 34:7	72:1,15 73:16 74:6
<b>second-</b> 230:3	265:15,16 269:1,2	257:9 266:22	<b>self-report</b> 124:18	74:19 75:9,15
<b>second-highest</b>	297:3,5,8 298:1,3	268:4 270:25	<b>selfie</b> 57:15	107:12 112:13
202:16	300:5,6 305:2,18	275:3 286:21	<b>sell</b> 35:21 149:14	158:7,9 162:5
<b>second-price</b> 202:14	316:1	287:10 290:15,20	181:16 201:22	218:8 266:25
<b>secondly</b> 211:8	<b>see</b> 5:25 12:1,16	290:23 293:7	306:9	271:5 284:13
253:16 260:13	18:12 21:20 23:17	301:10 303:2,9,20	<b>seller</b> 203:8	<b>sensor</b> 255:24,25
<b>seconds</b> 125:15	23:19,22 25:13,25	307:20 309:10	<b>selling</b> 40:8 42:22	<b>sensors</b> 255:12,12
186:1,2 248:19	26:1,19,20,21 27:6	310:25 315:1	120:24 203:8	255:13 257:17,19
257:12 312:14,24	27:17 28:20,21	<b>seeing</b> 4:25 114:17	247:15,22	292:11
<b>sect</b> 98:13	29:4 30:20,20	115:5 175:7 180:5	<b>semantically</b> 34:12	<b>sent</b> 53:9 108:18
<b>Section</b> 300:13	33:15 36:13 42:14	181:15 193:10,10	<b>semi-automated</b>	202:5 251:14
<b>sector</b> 5:22 38:5,15	43:10,24 44:21	193:25 207:18	85:5	253:12 254:6,16
38:16 242:12,17	45:10 51:5 52:3,12	215:17 286:12	<b>semi-automatically</b>	255:9 256:7
<b>sectors</b> 135:18 232:1	55:6 56:24 57:18	<b>seek</b> 7:7 179:21	274:1 281:22	<b>sentence</b> 159:3
<b>secure</b> 197:8 254:21	57:19 58:2 60:17	<b>seeking</b> 6:8 13:10	<b>semi-autonomous</b>	<b>sentences</b> 312:17
256:12,13,21,22	61:9,16,20 65:8,14	182:14	6:2	<b>sentiment</b> 233:8,19
257:5,9,11,21	67:7 69:8 70:6	<b>seeks</b> 19:14	<b>semifinal</b> 210:9	<b>separate</b> 157:16
<b>securing</b> 130:6	71:12 75:3 77:9	<b>seemingly</b> 137:20	<b>senators</b> 214:1	241:24
<b>security</b> 2:15,16	80:4 84:8 87:14	195:14	<b>send</b> 144:18 157:16	<b>separated</b> 48:9
3:11 4:1,23 5:9,13	88:25 89:1 112:19	<b>seen</b> 93:13 94:6 95:5	251:6	<b>separating</b> 224:12
5:21 7:2,5,15,21	116:15 117:17	126:1 220:21	<b>sending</b> 173:21	224:17
7:25 11:14 12:19	118:24 122:2,18	258:25 304:19	251:17 252:19	<b>sequence</b> 107:9
12:19 13:17 39:16	123:25 124:7	<b>sees</b> 73:1 118:3	255:13 258:11	280:11
39:17 63:11 113:7	125:10,22 128:25	181:22 204:1	291:14	<b>sequenced</b> 120:23
128:18,20 133:7,9	133:12 137:24	268:5	<b>sends</b> 257:21	<b>Serge</b> 68:16,18,20
133:13 171:20	138:19 141:20	<b>segment</b> 134:6	<b>senior-assisted</b>	80:11 111:17
188:2,6,12,19	148:8 158:21	166:12 168:10	158:17	112:7,13 237:7
189:8 191:3,23	159:11 162:11	<b>segmentation</b> 34:1,9	<b>senior-related</b>	<b>series</b> 19:16 62:23
194:25 195:8	171:14 174:6	37:23	158:17	141:2 293:9
196:17,22 197:9	175:9,11,12	<b>segmented</b> 34:10,10	<b>sensationalist</b> 56:16	<b>serious</b> 237:4
197:10,16 198:17	176:24 178:23	<b>segments</b> 59:19	<b>sense</b> 34:12 41:6	246:15
198:23 222:17	179:13,18,19	<b>segregate</b> 166:9	48:14 56:8,9,9,18	<b>seriously</b> 64:5,25
223:2,3,7,8,9,9	190:19,21 192:6,8	<b>select</b> 10:12 132:13	83:5,8,12,14 88:19	244:23,24,25
224:19 225:4	192:10,19,20,24	137:1,15 139:23	88:20 122:20	<b>serve</b> 33:3
226:18,23 227:3	193:12 194:3,5	<b>selection</b> 60:22	168:19 177:21	<b>served</b> 143:12
229:5 231:7 235:8	195:10,13 196:3,5	275:20 300:10	189:13,24 190:5	145:11 178:9,17
235:12 239:10,19	196:8,13,21 197:2	<b>selectively</b> 208:15	191:2 194:11	<b>server</b> 251:7 255:10

255:10,17	234:24 279:3	283:18 287:25	<b>shortly</b> 21:22 142:7	275:24 281:2
<b>serves</b> 7:18 194:18	281:17 302:24	297:10,11 303:4	145:25	283:5
<b>service</b> 19:11 106:8	306:8 316:7	305:14	<b>shot</b> 138:5	<b>shown</b> 31:20 79:9
109:19 121:11	<b>sets</b> 8:22 133:24	<b>shares</b> 127:10	<b>shots</b> 69:17 74:15,18	88:13 121:7
132:11 141:3,10	175:5 224:4	<b>sharing</b> 5:2 42:22	218:14	137:25 140:19,20
143:25 145:2	235:19 240:7	81:2 84:1,2 86:23	<b>shoulders</b> 35:15	141:3,12 144:6
151:23 152:15	294:13	91:2 104:2,3	36:4	158:13 261:6,8
154:21 157:11	<b>setting</b> 21:9,10	105:15 107:9,10	<b>shout</b> 134:8	262:14,24 263:2
162:3,19 163:13	28:21 101:16	109:16 110:2	<b>show</b> 18:10 20:7,25	263:16 267:13
224:21 262:25	181:9 212:12	113:12 126:13	21:1 23:3 24:18	268:11,12,13,14
263:5,8,9 271:14	241:13 289:20	200:1,10 209:15	28:3 35:2 44:7	268:21,25 270:1
272:16,17,22	<b>settings</b> 12:2 136:20	234:14 240:16	58:17 62:24 75:13	309:13
306:4	138:4,6,15 140:17	243:20 276:24	87:19,20 88:1,5,9	<b>shows</b> 14:24 15:22
<b>service-specific</b>	284:6,7,15,16	279:5 283:4 285:9	115:2 118:15	35:18 47:17 58:8
154:4	285:8 286:5 287:8	286:14,16,18,22	137:1,23 140:23	82:24 121:23
<b>services</b> 31:21 45:18	287:9 288:16,21	286:24,25 287:1	144:2 152:20,23	137:16 138:6
61:5 75:22 109:20	289:3,7,11,23	296:2 305:21	154:24 158:4,15	148:4 255:24
132:8,9,12 133:3	290:1,14,20 291:9	<b>Sharx</b> 254:2	181:16 202:12,17	261:17 270:9,25
149:25 151:5	291:11,15,19,20	<b>shed</b> 150:22 171:9	203:25 204:23	275:16 277:15,23
154:22 157:6	291:21 293:20,22	305:25 315:23	206:15 207:22	287:12 288:22
160:23 184:12	294:10,24 295:2	<b>sheds</b> 135:14	219:23 220:2,7	291:2
188:20 194:10,16	295:10,13 296:2,3	<b>shift</b> 16:13 18:9	227:21 229:9	<b>sick</b> 114:13 117:6
200:8	296:4 315:1	54:23 55:3	247:2 252:10	<b>side</b> 40:3 91:13,18
<b>serving</b> 145:12	<b>settle</b> 307:9	<b>shifting</b> 40:12	262:12 264:6,6,10	97:9 148:13,17
<b>session</b> 2:8,9,11,13	<b>settled</b> 232:23	<b>shifts</b> 56:7	264:10 265:6,19	173:23 193:12
2:14,16 8:11 14:1	<b>setup</b> 5:3	<b>SHMATIKOV</b>	267:7 270:6	201:21,23 237:19
67:19 68:1,4,8	<b>seven</b> 26:5 240:22	260:21 267:25	279:10 280:18	290:15
106:3 110:13	<b>Seventh</b> 1:10	305:12	281:7,10 282:11	<b>sides</b> 122:24 173:19
130:1 136:1,5,9	<b>severe</b> 271:11	<b>Shoenberger</b> 89:7	282:16 287:7	<b>sidestep</b> 243:7
186:20 188:1,5,11	<b>severity</b> 191:19	93:2 123:15	288:14,18 289:8	<b>sign</b> 90:21 122:2
249:13 250:1	<b>sexual</b> 158:8	124:14	301:24 309:5,6	<b>sign-on</b> 118:21
297:2,19 298:5,11	<b>shadow</b> 153:9,15,17	<b>shop</b> 5:24 36:23	315:19	<b>signal</b> 156:4 202:5
300:19	153:18 154:2	45:17 46:13 122:1	<b>showcase</b> 197:21	203:20
<b>sessions</b> 11:19 12:17	155:3,5 157:17	<b>shopped</b> 36:21	<b>showed</b> 15:24 31:25	<b>significance</b> 139:17
297:1	<b>shallow</b> 16:24,25	<b>shopping</b> 36:24	69:17 74:15 90:11	146:19 156:18
<b>set</b> 7:12 17:9 18:14	<b>shaming</b> 56:12	70:21 90:24	148:15 151:24	165:3
18:23 19:7 34:2	<b>shape</b> 40:14 195:23	266:17 267:3,11	152:22 154:10	<b>significant</b> 7:23 19:5
61:19,21 73:15	<b>share</b> 12:4,11 42:9	268:8,13,16	232:8 241:6	34:25 86:7,12 91:1
101:4 134:4	42:13 80:22 86:24	<b>short</b> 6:4 9:17 11:16	267:12	93:11 94:17
140:15 153:9	87:1 104:4 105:5,6	15:4 26:2 98:15	<b>showing</b> 44:22	139:18 140:20
157:14,16 166:4	105:7 110:1 112:5	105:21 185:14	71:17 82:7 85:13	147:5 166:13
169:6,11,13	139:1 141:1	264:5 272:12	90:15,19 141:16	179:2 189:7
170:17 183:18	208:15 211:19	273:18 290:18	148:9,13,16	191:22 193:17
186:16 215:6	286:10 288:7	<b>shortcomings</b>	158:25 184:13	260:24 262:20
217:18 223:21,24	<b>shared</b> 103:24,24	303:21,22	232:3,4,24 261:21	263:23 269:23
224:6,7 226:1,8,9	108:1 142:10	<b>shorter</b> 82:6 88:16	262:5 267:5,10	<b>significantly</b> 17:23
229:20 231:20	173:18 221:3	112:17 240:19	273:18 274:21,22	109:17 143:12

301:11	<b>single-topic</b> 148:12	<b>skimming</b> 224:25	94:15	52:25 119:18
<b>signify</b> 98:3	<b>Siona</b> 234:5 235:4	226:19	<b>snapshots</b> 253:10	190:13 247:19
<b>signs</b> 118:11	242:8 248:20	<b>skip</b> 32:24 90:3	<b>snippet</b> 58:18	<b>song</b> 108:7
<b>silence</b> 3:8	<b>sit</b> 218:23 220:17	94:20 228:5	<b>snoop</b> 263:24	<b>Sony</b> 230:24
<b>silly</b> 99:14	<b>site</b> 20:10,11,13	<b>skipping</b> 109:25	<b>snooping</b> 270:24	<b>sophisticated</b> 200:7
<b>SIM</b> 74:12	22:22 23:16,20,23	<b>slew</b> 127:8	<b>snow</b> 58:5	<b>sophistication</b> 52:7
<b>similar</b> 29:2,4,10	23:24 27:1 52:22	<b>slide</b> 30:19 44:22	<b>so-called</b> 37:20	295:7
32:1,10 46:21	61:9 95:3,3 96:9	122:6,21 191:20	188:23 231:21	<b>sorry</b> 5:1 27:23
53:18,19 69:23	125:5 150:1,2	283:12 290:15	<b>socially</b> 170:25	109:9 183:24
108:8 127:12	158:22 202:5	307:2	<b>social</b> 20:14 50:25	312:25
146:1 165:25	217:23 309:21	<b>slides</b> 32:25 236:9	90:24 91:24,25	<b>sort</b> 55:1 57:2,16
174:13 179:16	<b>sites</b> 22:5 23:10 24:8	247:11	92:1 93:20 95:25	65:20 85:9 97:16
206:7 207:23	24:9,13 25:1,19,23	<b>slightly</b> 270:25	135:1 160:23	111:16 116:17
239:18,25 261:18	26:11,14 27:25	<b>slink</b> 52:3	168:19 286:18	118:17 119:9,11
280:16	29:7,9,24 98:3	<b>slots</b> 144:25 145:3	302:6,17	122:18 123:8,17
<b>similarly</b> 76:15	118:23 126:13	<b>slowly</b> 116:12	<b>social/</b> 47:14	138:16 139:25
106:19 218:8,13	184:9 201:23	119:19 127:3	<b>socially</b> 146:10	141:19 157:15
<b>simple</b> 81:24 95:8	225:15,15 269:14	<b>small</b> 19:18 46:1,21	<b>society</b> 59:3,19	160:1,6,11,14,15
101:23 103:25	<b>sits</b> 306:12	56:16 98:13 109:7	150:14 209:18	160:17 161:7,10
132:1 148:12	<b>sitting</b> 138:16	155:24 186:14	272:9	161:13,17 162:1,4
154:5 155:1 241:1	251:25 253:4	216:16,17 233:16	<b>socioeconomic</b> 9:1	162:5,8,14,14,17
267:13 287:16	254:10 257:21	233:20 250:21	<b>soft</b> 79:19	163:25 164:8,8,15
288:17	<b>situation</b> 56:15	255:2 258:5 259:2	<b>software</b> 9:9 106:5	165:1,6,14,21
<b>simpler</b> 303:8	101:13 102:12	266:12 288:4,5	170:19 197:8	166:4,7,9,9,12,14
<b>simplified</b> 93:8	138:13 207:8	289:9 302:23	247:7,17 261:15	166:17,22,23,25
<b>simplify</b> 152:24	273:11	303:1	261:16 306:15,17	167:1,7,13,17
<b>simplistic</b> 154:6	<b>situations</b> 60:18	<b>smaller</b> 49:10	<b>sold</b> 108:17 263:18	168:5,7,9,18 169:2
<b>simply</b> 35:1 69:18	145:16 207:4,6	162:17 192:13	<b>solicited</b> 10:12	169:4,5,6 170:2,6
69:24 70:11 71:20	208:12 219:24	226:20 278:24	<b>solution</b> 54:8 63:2	170:15,19,23
71:23 101:2	289:22,24	295:6	79:8 241:1 243:5	172:9 173:17
103:23 212:12	<b>six</b> 17:18 60:7 68:10	<b>smart</b> 6:1 54:16	243:18 298:24,24	177:6 179:7
293:4 305:23	109:8,9 245:21	62:10 250:13,18	307:11	182:22 213:3
<b>simulate</b> 139:8	276:11 289:15	251:5 252:9,12	<b>solutions</b> 10:8,10,14	214:11,14 220:10
<b>simulated</b> 139:11,15	290:19	258:3,5 259:25	54:19 132:5	241:8,9 245:16
140:15 141:4	<b>six-item</b> 91:25	284:8,9 286:1	242:24 273:23	246:23 284:4
143:13	<b>sixth</b> 125:25	289:12 292:6	299:4,11	299:16 307:10,22
<b>simulating</b> 139:9	<b>size</b> 168:6 175:22	<b>smarter</b> 122:13	<b>solve</b> 55:10 161:18	308:3 311:13
204:24	<b>sizes</b> 166:11	<b>smartphone</b> 127:9	162:21 298:23	312:1,8
<b>simulations</b> 204:25	<b>skeptical</b> 35:24 36:1	<b>Smartthings</b> 257:2	<b>solving</b> 307:13	<b>sorts</b> 150:3 174:2
207:14	96:11	257:15,17,19,23	<b>somber</b> 57:2	224:25 228:12
<b>single</b> 28:17 29:16	<b>skepticism</b> 95:4	<b>smartthings.com</b>	<b>somebody</b> 172:8	232:17 263:19
53:1 118:21 125:8	<b>skews</b> 117:19	257:13	253:2,4,5,19 256:2	283:16 293:6
172:7 214:21	<b>skiing</b> 53:8	<b>smattering</b> 228:16	266:19 301:22	<b>sought</b> 104:10,12
232:7 276:19	<b>skill</b> 101:4	<b>Smith</b> 234:4 241:3	302:21 307:17	<b>sound</b> 3:21 44:23
278:25 281:12	<b>skilled</b> 276:10 277:4	242:6	<b>someone's</b> 122:6	51:3 131:5 258:1
312:5	277:17 278:8	<b>SMS</b> 287:2	125:11	<b>sounds</b> 53:3
<b>single-family</b> 270:16	<b>skills</b> 30:13	<b>Snapchat</b> 9:4 57:16	<b>somewhat</b> 32:9	<b>source</b> 30:18 116:25

117:1 139:1 165:11,13 170:19 <b>sourced</b> 114:8 <b>sources</b> 225:13,18 <b>space</b> 54:1 100:11 102:5 103:2 131:11,23 142:11 145:21 201:22 283:21 284:20,25 293:16 294:1 295:14 296:13 304:3,18,22 305:16 <b>spaces</b> 292:6 <b>spam</b> 229:1 <b>Spanish-speaking</b> 45:4 <b>spans</b> 240:20 <b>sparse</b> 156:4,6 <b>sparsity</b> 156:1 <b>speak</b> 7:14 222:1 <b>speaker</b> 252:12 302:12,14 303:3 <b>speakers</b> 12:16 142:7 302:20 303:11 315:15 <b>speaking</b> 191:25 306:20 <b>speaks</b> 238:1,3 <b>specific</b> 46:25 87:11 87:15 100:15,16 119:21 127:23 128:1 133:13,20 134:9 143:24 147:3 151:20,21 157:6 158:12 168:3 169:24 197:25 200:24 201:16 208:10 301:7 <b>specifically</b> 96:18 148:8 154:10 157:2 158:6,16 200:3,18 201:13 204:10 205:13 228:23 236:3 <b>specified</b> 87:1	<b>specify</b> 164:8 293:9 <b>spectacular</b> 60:24 <b>spectrum</b> 302:12,19 <b>speculating</b> 220:19 <b>spelling</b> 318:20 <b>spend</b> 34:23 171:17 <b>spending</b> 110:14 <b>spent</b> 237:22 301:14 <b>sphere</b> 126:17 131:19 <b>spheres</b> 239:5 242:1 <b>Spiderman</b> 117:25 <b>spike</b> 195:14 196:21 <b>spiky</b> 195:10 <b>spillovers</b> 212:9 <b>spin</b> 177:8 <b>split</b> 84:1 166:1 176:6 278:22 279:1 302:3 <b>splitting</b> 278:24 <b>spoke</b> 255:16 316:3 <b>Spokeo</b> 64:4,5 <b>spoof</b> 9:25 <b>spouse</b> 158:22 <b>spread</b> 103:9 276:24 <b>sprouted</b> 134:19 <b>spur</b> 7:4 10:9 133:16 <b>spurious</b> 218:18 <b>SSRN</b> 210:8 236:10 <b>staff</b> 3:16 31:15 130:17 314:5 <b>stage</b> 7:12 14:12 154:7 171:5 220:22 <b>stages</b> 43:20 124:15 154:1 215:16 235:16 270:9 <b>stake</b> 263:13 <b>staked</b> 65:3 <b>stakeholders</b> 8:4 200:20 201:4 209:12 272:21 304:4,11 305:8 <b>stalking</b> 22:23 <b>stamp</b> 73:21 <b>stand</b> 186:22 <b>standard</b> 89:14,21	89:21 215:20 222:19,22 238:6 258:8 271:2 277:6 287:13 <b>standards</b> 56:14 89:9 223:1 258:3 260:6,10 305:5,5,6 <b>standing</b> 35:14 36:3 64:23 151:16 <b>standpoint</b> 88:7 <b>Stanford</b> 110:18 272:10 <b>Staples</b> 160:18 162:7 182:11,12 183:2 <b>Staples'</b> 160:11 <b>stars</b> 37:18 57:6 <b>start</b> 11:18 15:11 30:25 31:14 39:9 39:13 52:5 68:4,18 80:18 90:2 110:19 114:13 141:16 148:4 165:10 171:2 198:21 205:4 235:3,4 236:5,23 242:16 287:11 298:6 299:5 309:21 310:10 <b>started</b> 16:5 36:11 39:15,21 69:15 128:5 136:15 137:8 145:12 152:14 176:13 209:2,3 236:13 275:13 292:4 313:22 317:4 <b>starting</b> 21:17 36:16 43:14 58:19 62:23 170:18 185:15 236:16 313:2,9 <b>starts</b> 61:8 165:9 <b>startups</b> 242:25 250:21 <b>state</b> 2:9 11:19 14:2 14:10 16:10 19:22 21:9 57:3 105:8	188:7,14 213:19 214:1 215:22 216:4,11,19 218:4 218:12,18 220:9 228:9 250:12 <b>stated</b> 79:18 103:23 <b>statement</b> 158:5 212:21 <b>statements</b> 46:13 48:8,9,14 85:10 106:8 191:17 <b>states</b> 1:1 85:18 98:25 189:3 213:23 220:21 221:1 228:2 234:19,21,22 <b>stating</b> 114:25 <b>statistic</b> 140:4 <b>statistical</b> 48:18,22 49:22 139:17 146:19 147:23 156:17 162:12 165:2 170:23,24 172:25 174:3 177:19 195:23 216:1,21 221:17 230:21 315:13 <b>statistically</b> 86:7 104:17 139:18 140:20 179:2 <b>statistics</b> 154:18 164:23 177:17 <b>status</b> 76:3 273:17 <b>statutory</b> 228:13 <b>stay</b> 15:2 32:25 113:6 132:11 <b>steady</b> 228:23 <b>steak</b> 116:22 <b>stealthily</b> 263:25 <b>step</b> 13:12 133:22 142:23 146:4 246:17,20 279:16 288:23 290:4 292:3 <b>steps</b> 29:20 247:24 <b>Steven</b> 20:2,4 31:10 62:19	<b>Steven's</b> 52:9 <b>Stevenson</b> 110:17 114:22 122:5 <b>stewards</b> 62:9 <b>stick</b> 135:3 <b>sticking</b> 222:8 <b>Stigler</b> 236:15 <b>stockpiled</b> 195:17 196:24 <b>stood</b> 214:19 <b>stop</b> 59:19 117:21 118:4 142:24 146:12 179:14 181:22 243:19 250:17 313:19 <b>stopped</b> 22:5,11 29:8 36:11 <b>storage</b> 16:20 17:23 17:24 18:1,5,11 26:16 109:16 264:22 265:3,5,8,9 265:13,19 267:6 267:15 268:20 297:10 <b>store</b> 18:6 45:13,17 46:13 47:19 58:16 59:7,8 160:12 180:16 183:5 265:13 266:17 <b>store's</b> 45:15 <b>stores</b> 51:7 260:24 267:5 <b>stories</b> 56:16 <b>story</b> 53:9 57:16 62:5 223:4 287:10 287:11,14 290:17 295:3 <b>strands</b> 297:20 <b>Strange</b> 36:23 <b>stranger</b> 90:12 <b>strap</b> 163:22 <b>strategic</b> 208:14 <b>strategically</b> 207:10 <b>strategy</b> 204:17 296:16 <b>strawman</b> 60:10 <b>stream</b> 254:8,10,11
---	---	--	--	---

254:12	16:7 24:17 27:11	162:17	217:21 218:11,14	59:8 65:6 66:12
<b>streams</b> 253:8	30:6 37:14 38:11	<b>subscribers</b> 10:17	221:21 291:23	94:1 98:23,25
255:21	69:22 72:11 73:9	<b>subscripts</b> 216:6	<b>suite</b> 163:3	113:22 114:3,5,6,7
<b>street</b> 1:10 3:22,23	83:21 84:17 87:16	<b>subsection</b> 193:11	<b>suits</b> 228:18	119:10 162:13
7:6 62:22	88:19 95:2 96:15	<b>subsequently</b> 202:6	<b>sum</b> 170:21 220:12	163:7 177:6
<b>strict</b> 228:14	98:22 111:20	<b>subset</b> 155:24	<b>summaries</b> 273:18	178:11,11,12,14
<b>strident</b> 213:12	115:23 118:20	<b>subsets</b> 56:16	<b>summarize</b> 208:8	182:1 246:3
<b>strikes</b> 238:21	127:7,11 157:24	153:11 154:2	<b>summary</b> 41:7	256:18 264:17
<b>string</b> 27:21	157:25 159:8	<b>substance</b> 141:14	146:12 264:5	280:23
<b>striving</b> 110:24	160:10 188:8,25	147:6,6	<b>summer</b> 73:9 271:8	<b>surface</b> 13:3 194:11
<b>strong</b> 7:17,18 48:18	189:5,12 197:18	<b>substantial</b> 37:16	281:20 290:5	<b>surplus</b> 204:20
63:11 78:6,15	197:23 199:12	38:19 134:13	<b>Sunlight</b> 145:25	205:1 209:13
108:10 122:15	213:18,22 214:5	193:14	147:21 151:18	<b>surprise</b> 73:4 93:12
162:18 164:2,9	215:3 217:14	<b>substantive</b> 31:17	152:1,2,10,14,23	95:24 217:12
168:15,15 198:11	220:14,15,22	131:3	153:24 154:5,9,16	284:5 285:25
273:4 304:20	237:15 247:2	<b>subtle</b> 271:6	156:8,14,19 157:2	306:24
<b>stronger</b> 144:15	252:3,3 269:24	<b>success</b> 152:5	157:2,8,21 166:1	<b>surprised</b> 21:23
<b>strongest</b> 57:21	270:4,20,22 271:7	270:24 283:7,8	173:23 175:3,23	283:16,24
<b>strongly</b> 45:24,25	283:20 290:19	286:10 309:23	176:4	<b>surprising</b> 50:11
59:24 144:15	291:2 302:6,6	<b>successful</b> 65:6	<b>supermarket</b> 46:6,7	140:23 217:18
243:17 289:21	<b>studying</b> 115:17	<b>sudden</b> 141:16	46:18,24,25 47:2	<b>surveillance</b> 19:5
292:1 312:19	122:17 157:5	<b>sue</b> 64:24 65:1	47:10,24 48:24	<b>survey</b> 37:6 39:5
<b>struck</b> 130:25	250:13	<b>sued</b> 64:10	49:9 50:14,14	41:11 45:1,5 58:8
<b>structurally</b> 262:17	<b>stuff</b> 41:5 43:19 48:6	<b>suffer</b> 227:10,23	<b>supermarkets'</b>	69:16 77:14 84:17
<b>structured</b> 132:25	50:2 62:6 182:13	228:3 231:16	48:20	91:13,14,18,21
<b>student</b> 250:6	298:16	232:7	<b>supplies</b> 157:14,21	98:22 233:5,6
<b>students</b> 68:23	<b>subassembly</b> 193:11	<b>suffered</b> 96:3	<b>supply</b> 217:23	314:20
134:18,21,25	<b>subconsciously</b>	227:17	263:16 264:25	<b>surveyed</b> 12:7
151:15 183:23	111:6	<b>suffering</b> 209:16	<b>supplying</b> 263:1	<b>surveying</b> 16:5
276:7,11 277:11	<b>subject</b> 106:6	225:6 231:22	<b>support</b> 7:2 49:11	<b>surveys</b> 19:16 37:1
279:16,21	<b>subjective</b> 119:18	<b>sufficient</b> 34:7	61:18 66:15	38:7 44:7 93:18
<b>studied</b> 84:18	<b>subjects</b> 119:6	242:22 271:4	273:21	133:1 220:8
125:23 261:22	200:12	273:22 295:1	<b>supported</b> 115:9	230:15
<b>studies</b> 26:24 30:10	<b>submissions</b> 10:13	298:22	262:2	<b>susceptibility</b> 215:9
35:2 36:10,14	191:8 195:20	<b>sufficiently</b> 310:4	<b>supporter</b> 268:19	<b>suspect</b> 304:3 310:6
38:13 41:21 66:11	<b>submit</b> 30:21 190:1	<b>suggest</b> 50:7 57:8,10	<b>supporters</b> 49:10	310:11
83:11,11 93:19	190:1 202:13	97:17 161:20,23	<b>supporting</b> 200:15	<b>suspicious</b> 3:25
94:6 95:5 115:2,7	<b>submits</b> 261:5	227:5 233:21	200:16 286:11	<b>Suthers</b> 105:10
116:15 118:15	<b>submitted</b> 144:1	242:11	<b>supports</b> 64:23	<b>symptoms</b> 167:9
121:7 142:8	191:11 192:6,12	<b>suggested</b> 15:19	283:6	<b>sync</b> 43:23
157:12 210:21	192:15,21 193:15	49:12 50:19	<b>suppose</b> 137:22	<b>syndication</b> 263:18
235:2 238:24	193:20 194:23	102:19 182:24	<b>supposed</b> 44:21	<b>synthesize</b> 314:14
239:4 240:20	195:4 196:2	300:20,22	117:11 254:9	<b>synthetic</b> 108:3
241:25 275:4	<b>submitting</b> 195:16	<b>suggesting</b> 178:15	264:18 286:21	<b>system</b> 3:19 55:8
276:4 281:19	<b>subpopulation</b>	289:19 299:11	308:23	56:13,20 69:3,7
308:24	168:14	<b>suggestions</b> 8:16	<b>supposedly</b> 89:18	71:1 73:11 75:10
<b>study</b> 11:4 12:1,12	<b>subpopulations</b>	<b>suggests</b> 41:24 79:7	<b>sure</b> 14:14 33:19	75:25 76:10 99:24

101:18,20 103:7	244:22,24,25	260:22 266:1,11	218:12,15	39:2 57:5 59:25
105:14 126:19	252:3,25 266:14	272:3 298:20	<b>taxi</b> 60:13	64:7 110:16
136:24 137:5	278:7 301:18	299:22 301:14	<b>Taylor</b> 210:9	119:19 120:18
138:21,24 139:3	308:3,5 312:24	<b>talks</b> 176:6 188:11	<b>teach</b> 44:18 171:16	127:3 131:8
140:7,13 143:18	<b>takeaway</b> 190:25	258:25 261:23	171:19,19,20	134:14,21 146:9
143:22 145:15,22	192:23 194:13	302:4,4	<b>teaching</b> 52:2	176:11 188:13
146:1,21 147:15	226:21 231:12	<b>tangible</b> 12:12	<b>team</b> 4:22 11:3	201:17 211:7,9
151:19 169:1	<b>taken</b> 71:9 74:18	<b>tap</b> 6:19	31:20,22 67:9	215:15 243:17
170:3,5,8 175:16	123:14 129:4	<b>target</b> 116:6,17	197:9 225:14	281:16 288:17
217:13 224:22	245:22 318:8	144:12 148:6,8,21	275:1,2 283:11	290:5 295:12,17
289:5 292:25	<b>takes</b> 70:5 163:11	149:5 151:23	<b>tech</b> 6:24 7:8 9:2	309:22,23 310:19
<b>systematic</b> 139:18	167:22 169:8	158:7,11,18,19,24	11:11 159:23	<b>Technology-focus...</b>
<b>systems</b> 44:12 56:21	238:9,13 267:4	202:25 230:23	260:20	134:19
71:3 79:10,13,20	293:11	<b>targeted</b> 47:5	<b>technical</b> 8:13 10:12	<b>technology-related</b>
79:24 101:25	<b>takeup</b> 210:25	107:22,23 144:23	10:19 30:11 32:6,6	11:7
131:20 138:23	215:17	146:19 147:7	132:6 166:15	<b>Teeing</b> 301:25
142:3 145:7,9,20	<b>talk</b> 21:3,3 24:5 26:9	148:9 149:3	172:19,24 190:8	<b>telemarketing</b> 229:2
146:3 147:14	32:20,20 35:24	171:11 192:17	264:1 271:1,20	<b>telephone</b> 41:11
151:17 172:5,18	41:6 43:20 44:10	199:15 200:19	303:19	<b>tell</b> 24:22 61:23 62:5
172:20,25 173:1	44:21 51:6,17	201:9 209:18	<b>technically</b> 264:14	126:15 148:1,20
175:17,21 222:19	65:10,12,20 80:15	211:12 241:20	<b>technique</b> 22:9 23:8	149:1,9,13 151:10
230:7 294:7	91:14 92:25	243:3	28:4 29:5,12 198:1	157:1,9 159:21
296:17 315:18	100:14 103:11	<b>targeting</b> 142:13,13	<b>techniques</b> 8:12	166:25 169:2
	105:23 124:6	143:10,18 144:9	85:5 173:1,13	185:3 222:20
<b>T</b>	126:1 145:24	144:21 147:5,22	174:3 215:20	234:17 260:5
<b>T</b> 318:1,1,1,17,17	151:9,25 152:23	148:20 149:10	<b>technological</b> 6:17	269:25 283:16
<b>table</b> 47:17 194:1	164:18 176:7	151:20,25 152:5	9:23 10:10 13:4	298:21 307:20
<b>tackles</b> 200:17	186:15 188:15	152:24 153:5,19	44:11 63:22	313:13 315:18
<b>tag</b> 160:24	199:1 214:18	154:8,15,19 155:4	242:24	<b>telling</b> 151:16
<b>tagged</b> 56:6 161:3	224:11,16 235:5	155:7,19 156:12	<b>technologies</b> 6:9 8:5	216:13
<b>tagging</b> 160:22	235:15 243:16	157:4,12,15,19,22	11:4 16:12 17:21	<b>tells</b> 149:2 277:21
<b>tags</b> 163:13,20	250:14 251:9,9	157:24 159:8,9,10	20:23 23:22 24:19	<b>temperature</b> 255:12
<b>tail</b> 258:5	252:23 255:3,7	160:4 175:6,7,8,10	26:3 52:13 57:12	<b>ten</b> 296:6
<b>tailored</b> 297:8	257:2 271:19	175:11 201:12	60:12 119:21	<b>tend</b> 93:14 106:16
<b>take</b> 13:13 22:20	283:4 298:11	202:3 204:5	127:1,24 128:2	121:22 180:22
26:4 28:15 47:1	302:12 304:7	205:19 206:6,25	209:14 220:24	206:4,12,15 207:2
53:2 57:15 64:3,5	<b>talked</b> 21:15 44:6	<b>targets</b> 148:25	243:15 244:4,10	207:24 285:16
64:24 68:3 89:19	53:18 62:4,19,20	153:21 155:24	315:12	<b>tendency</b> 299:19
94:19 101:3	88:7 111:12	158:14,21	<b>technologist</b> 13:1	<b>tends</b> 116:11 219:19
106:18 117:23	212:18 241:21	<b>task</b> 138:23 162:25	313:22	234:15 306:25
128:18 130:15	259:17,19 275:6	167:10 278:23	<b>technologists</b> 8:3	<b>Tene</b> 15:5 57:1 63:5
137:2 142:17	299:12,14 300:2	279:9	9:22 11:3 134:22	63:7 65:2
159:2 161:20	<b>talking</b> 20:6 42:7	<b>tasks</b> 275:24,25	243:19	<b>tensions</b> 295:21
175:21 178:7	50:2 53:6,8 73:17	278:2,3 279:1,11	<b>technology</b> 3:5 4:21	<b>tenure</b> 211:24
189:12 193:2	99:17 100:22,23	<b>Tasmania</b> 100:8	6:4 9:25 10:22,24	<b>term</b> 59:4
195:9 198:5	114:17,18 136:23	102:15	14:7 16:14 17:24	<b>terms</b> 46:5 57:21
215:12 222:19	243:16 255:16,22	<b>tastes</b> 116:6 203:14	18:9 21:21 23:20	59:11 65:21 90:22

90:23 92:18 94:11 104:21 105:23 106:6,7,8,8 108:6 108:11,12,24 109:2,6,12 121:12 121:12,17,18,25 141:25 164:25 165:23 198:12 205:1 213:17 216:14 217:16 236:24 237:1 240:5 244:11 259:18 300:17 304:8 306:7,11 <b>terribly</b> 140:22 <b>terrific</b> 58:20 59:3 59:17 <b>test</b> 88:16,23 98:12 101:19 105:12 109:24 121:4,6,9 125:8,10 139:16 148:8 166:3 173:23 195:23,24 211:18 215:5,7,10 215:12,22 216:15 216:24 217:9,19 218:6,7,9 219:1,20 219:25 220:2 221:6 302:15 308:6 <b>tested</b> 44:16 76:24 218:4 <b>testing</b> 100:11,16 101:13,15,16,17 102:3,19 109:23 124:16 125:24 126:11 146:3 156:16 159:19 161:11,11 163:3 173:20 210:18 211:1 213:7 218:22 221:3 234:19,22,23 <b>tests</b> 104:25 106:1,1 106:12 108:17 120:16,19 213:5 215:1 217:7,17	221:11,12 302:13 308:3 <b>text</b> 27:1,2,15,20 29:3 34:9 252:20 253:13 254:6 255:6,8,9 256:6,6 256:23 257:6 275:18,20 285:18 285:20 310:11 <b>textual</b> 81:1 82:4 <b>thank</b> 4:17,19 5:16 13:11,17,21 14:3,4 19:23,24,24 31:8 31:10,18 40:17 41:4 51:24 57:1 63:7 67:17 68:21 80:11,15 89:3,5,11 100:4,13 110:10 110:12 113:11,15 114:21 122:4 128:3,24 130:9,10 130:16 135:21,24 136:3,21 147:17 147:19 159:12,13 171:3 186:20 199:2,4,7 200:23 208:19 210:13,15 210:19 221:24,25 222:3,8,8 233:22 233:25,25 249:12 249:13 260:16,18 282:19 296:23 312:25 313:24 314:2,4,10 317:5 <b>thanked</b> 256:25 <b>thanking</b> 31:14 <b>thanks</b> 41:1 51:22 51:24 62:1 113:15 159:20 241:2 242:6 250:8 271:23 298:8 301:19 303:13 <b>theft</b> 107:22 224:21 <b>theme</b> 32:2 54:22 112:1,10 235:9,21 <b>themes</b> 68:13 111:9 171:14 174:7,10	235:6 271:21 <b>theorem</b> 140:3 <b>theoretical</b> 32:23 <b>theoretically</b> 65:22 155:21 <b>theoretician</b> 155:20 <b>theories</b> 40:1 295:22 <b>theory</b> 32:11,24 33:1,2 52:17 235:19 <b>Thermostat</b> 252:14 255:4 256:11,13 <b>thesis</b> 33:2 <b>thing</b> 22:8 24:11 28:18 36:18 46:18 54:5 59:11 63:14 75:23 98:7 101:7 101:14 109:4 120:17 121:4 126:24 130:25 137:21 138:11 161:23 162:10 173:7 176:8 185:23 195:13 214:9 216:22 218:1 232:8 241:14 246:14 252:22 255:14 257:4,8,15 258:13 258:20 265:9 266:1 267:21 270:7 278:22 280:4 300:12,14 <b>things</b> 7:24 21:25 24:6,17,23 25:20 25:24 26:11,18 27:19 28:3,24 29:4 32:1 39:13,14 40:22 41:16 42:6 47:6 48:4 51:6,20 51:21 53:24 58:20 58:24 59:3,4,18,20 60:1,22 61:24 67:10 72:1,10,21 73:17,18,19,21 77:20 79:1 81:25 82:2 90:2 99:16	101:23 104:1 107:1 108:22 111:1,22 117:10 126:4 127:5,17,18 133:14 136:15,18 137:2 138:3,15 141:22 149:18,20 149:21,23 153:8 154:15 156:20 158:3 160:25 163:16,18 164:11 164:14 166:10,11 167:10 172:9 173:15 180:12 181:12,18 182:19 218:17 239:19 242:8 249:1 250:10 254:19,23 258:15 259:8 261:24 266:23 271:3 284:24 285:20 296:12 298:9,18 299:14 299:20,22 302:2 303:5 306:23 307:1 313:17 314:12 315:10 316:23 <b>think</b> 28:13 29:22 30:1 31:18 35:10 35:11,19,20 36:13 36:14,24 40:5 43:22 45:9 46:6 47:5 51:4 53:17 55:11 56:7 57:1,18 58:2,5,7,14,22 59:2,14,18 60:9,23 61:7,11,17 63:7,8 63:11,14,20,22 64:2,16,19 65:2,3 65:4,14,25 67:5,11 84:13,14 86:20 99:8 100:8 102:13 102:14 104:11,22 107:3,6 110:5,7,25 115:1,9,22 117:8 117:10,16 118:4,8	118:11 119:10,12 119:19,20 121:22 121:23 122:5,7,8 122:10,12,14,21 122:22 123:6,8,14 123:21 125:11 126:4 127:6,22 131:15,22 132:1 134:22 142:23 148:22 155:15 162:21 167:18 168:10,17 169:7 171:1,24,25 172:1 172:4,9 173:3,5,18 173:20,22,24 174:4,9,13 175:13 175:14,18 177:11 177:12,13,15 178:9,14,17,25 179:4,10,24 180:11 181:3,11 181:14 182:7,8,16 183:3,18 184:2 185:12 198:24 199:20 207:7 211:3,6,9,14,15 212:4,6,11 214:11 214:24 215:25 216:3 218:8,18 219:7 220:1,13,25 222:23 223:1 224:18 225:1,4 227:12 229:11,12 229:19 231:11,23 232:2 235:8,17 237:22,24,24,25 238:12,14 239:15 240:25 241:9 242:3,18 243:8,14 244:14,14 245:8 245:11,18 246:9 246:13,17,18 247:3,25 248:2 250:16 255:1 264:15 273:9 282:25 283:13 284:5 285:14
--	---	---	--	---

293:3 294:18,21 295:15 296:22 300:1,15,18 301:9 302:5 303:17 304:23 305:8,12 308:9,11,12,16 309:18,19 310:24 311:15,20 312:10 312:18 313:1,15 313:16 314:16 315:4 316:6,25 <b>thinkers</b> 13:16 <b>thinking</b> 11:13 13:6 42:16 51:7 54:16 56:4 103:3 123:9 126:13 181:1,23 185:22 211:12 243:23 <b>thinks</b> 85:19,25 <b>third</b> 12:9 18:13 20:12 35:22 77:18 82:18 110:3 112:6 112:10 144:5 146:22 149:25 153:18 216:14 225:22 254:25 262:10 292:23 302:20 <b>third-party</b> 18:15 18:17,23 19:7 73:12 189:15 230:3,9 <b>thought</b> 92:22 95:11 104:15 113:17 114:19 144:11 186:3,4 214:13 231:23 265:25 298:8 299:3 <b>thought-provoking</b> 113:18 <b>thoughtful</b> 131:4 <b>thoughts</b> 15:6 54:18 67:14 113:12,14 235:4 236:7 248:20 298:4 <b>thousand</b> 18:1 103:12,12,13,14	177:22,24,25 178:6 282:4 <b>thousands</b> 52:11 79:22 133:15 155:8 <b>threads</b> 274:15 <b>threat</b> 62:16 <b>three</b> 11:16 17:19 19:17 35:4 37:18 45:21,22 46:12 57:20,20 72:11 111:9 116:14 127:7 136:12 152:2,25 153:7,8 153:10 155:2,3,4 171:8,15 173:11 194:3 195:13 202:20 203:16 209:2,8 214:5 229:7 234:20 236:12 257:12 262:23 274:25 284:11 290:11 312:19 <b>three-dimensional</b> 132:24 <b>three-item</b> 92:21 <b>three-players</b> 201:9 <b>three-prong</b> 97:15 <b>three-quarters</b> 291:7 <b>thrilled</b> 57:11 130:7 133:12 <b>throw</b> 177:5 <b>THURSDAY</b> 1:6 <b>ties</b> 11:11 <b>tight</b> 14:17 <b>tightly</b> 274:14 <b>time</b> 13:8 14:24,25 15:8 21:16 25:15 28:20 32:25 34:23 41:23 51:13 53:16 53:21 60:18,21 64:17 67:17 69:25 70:16 71:19,25 72:2,2,13,25 73:11 73:16,21 74:25	76:4,9,19 77:4,4 77:14 78:10,12,20 78:21,22,25 93:9 94:25 109:7,11,12 109:12,12 110:4 110:13 116:10,22 118:4 120:10,25 121:10 123:4,8 125:20,24 126:2 127:5 128:4,7,18 132:14 140:9 141:21 142:3 150:15 151:11 163:6 170:1 192:20 195:4 196:5 203:6,17 204:21 212:23 213:1 227:21 236:17 237:22 239:13 240:20 242:19 243:15 263:18 264:9 267:7 268:15 269:24 274:8 276:14 282:6 284:7 285:6 286:7 286:20 296:22 301:14 303:11,15 308:2 310:20 313:25 314:3 <b>timeliness</b> 233:14 <b>times</b> 18:1 20:10 29:7,8 62:16 118:7 137:9,16 140:19 141:18 167:8,12 167:22 170:17 178:7 211:20 241:25 302:9 <b>Tina</b> 3:4 4:19 <b>tinier</b> 285:19 <b>tiny</b> 285:18 <b>title</b> 235:7 318:3 <b>titled</b> 136:19 147:21 159:17 <b>toasters</b> 53:25 <b>today</b> 3:16 4:3,24 5:22 7:18 11:15	13:2,11 15:21 20:5 21:1 31:16 32:10 32:20,25 39:5 40:20 43:5 52:3 57:3 62:17 66:23 91:14 100:9 103:11 113:16,20 130:7 134:10,12 136:5 199:12 200:17 210:23 241:21 260:22 261:22 292:17 294:7 296:15,25 298:13 302:4 304:17 305:16 306:4 312:19 316:17 <b>today's</b> 4:16 5:5 6:21 8:7 13:15 39:25 130:25 148:4 <b>tohe</b> 14:17 <b>told</b> 128:22 159:5 219:13 244:3 256:24 265:17 267:12 271:17 <b>tolerance</b> 232:21 <b>ton</b> 270:14 303:10 <b>tons</b> 284:6,6 <b>tool</b> 9:15 30:4,7 157:23,24 159:22 163:2,5,22 164:3 166:22 170:8 185:19 186:10 275:14,16 316:7 <b>Toolkit</b> 159:19 <b>tools</b> 10:8 26:19 29:11,11 30:3,10 61:12 92:14 132:2 132:13,21 142:1 148:1 150:21 157:5,7,9 159:6,7 162:23 170:24 171:9,23 172:10 174:2,20 175:14 182:18 184:17 185:20,23 247:17	312:9,12 316:3,5 <b>top</b> 11:18 13:16 16:21,21,21 17:13 18:21 19:3,4,9,9 24:12 28:2 29:1 31:3 76:3 157:4,8 194:1 195:13 278:11,11 <b>topic</b> 137:3 188:15 <b>topics</b> 11:16 12:17 158:12 235:10 <b>total</b> 18:12 84:18 198:6 227:13,22 228:19 229:17 <b>totally</b> 257:5 267:10 268:12 306:5 <b>totals</b> 226:12 <b>touch</b> 245:19 <b>touchstone</b> 179:4 235:10 <b>touchstones</b> 177:13 <b>tough</b> 303:25 <b>track</b> 16:6 18:7 19:10 21:18 23:11 31:22 95:12 116:12 150:25 172:6 <b>tracked</b> 15:17 32:5 61:16,20 315:11 <b>tracker</b> 21:13 <b>trackers</b> 22:16 23:10 136:24 137:19,19 139:1 <b>tracking</b> 7:25 8:9,10 8:12 12:23 15:25 16:2,11,13,13,14 16:15,16 17:11,12 17:22 18:4,9,10,20 19:1,2,6,15,19 20:22 21:6,8 23:12 23:20,22 24:14 26:3,21,22 28:5,12 43:18 50:22 52:8 53:24 54:12 61:2,4 61:6,24 62:24 65:22 182:25 315:12
--	---	--	--	---

<b>tracks</b> 125:21	<b>transmission</b> 177:12	<b>truly</b> 38:23 291:23	287:5 291:10	154:1 157:1 166:2
<b>traction</b> 65:7	<b>transparency</b> 20:7	294:2	305:5,7,8 314:14	173:19 174:11
<b>trade</b> 1:2,8 5:19	20:25 23:17 24:4	<b>trust</b> 42:21 56:2	<b>Tschantz</b> 136:16,21	176:9 178:21
31:14 39:20,21,23	42:23,24 54:24	62:1 66:7 91:25,25	136:22 179:8	182:19,23 185:19
97:7 108:15 111:5	55:9,12 56:1,12,23	92:1 93:20 94:3	186:4	188:11,24 189:12
151:4 188:4 234:5	62:17 71:10 75:13	95:25,25 97:8 98:4	<b>Tucker</b> 210:16,19	189:18 190:12
318:9	120:11 148:3	99:23 111:8	210:20 236:25	191:17,22 194:7
<b>tradeoff</b> 32:20 35:24	150:21 151:8,12	156:13 272:18	238:19 241:12	196:3 197:17
35:25 41:3,12	157:3,5 159:6	307:16,17 309:12	245:7	198:7 201:25
43:17 46:22 48:24	174:25 175:17	<b>TRUSTe</b> 95:9	<b>Turk</b> 84:19 276:8	203:12,18 205:15
49:10,11	237:5,19 305:12	<b>trusted</b> 55:8 92:2	<b>turn</b> 3:22 54:6,21	206:8 207:3,5
<b>tradeoffs</b> 32:21	306:6,19,25	263:20	58:11 113:13	222:13 234:9
37:21 41:9,15,17	307:10,15,15,17	<b>truth</b> 75:3 244:3	171:13 235:3	241:24 251:8
42:7 43:3 44:4	308:12,15,18	<b>try</b> 14:16,22 15:2	241:3 293:12	273:5 274:17
45:8,9 46:1,2	309:11,14,16	27:16 45:1 49:1	<b>turned</b> 160:13	295:15 302:10,18
48:19 49:3,6,15	315:5,16	69:3 77:22 79:13	<b>turns</b> 46:15 48:13	303:2 312:17
50:21 306:23	<b>transparent</b> 31:6	121:16 128:23	76:6,17 148:25	<b>two-way</b> 7:6
<b>trades</b> 210:1	<b>travel</b> 152:7	160:24 161:13	155:16 173:11	<b>tying</b> 240:6
<b>Trading</b> 121:14	<b>travels</b> 103:6	162:10 163:5,24	266:4 268:10,17	<b>type</b> 7:9 21:8 39:17
<b>traditional</b> 10:7	<b>treated</b> 34:4 186:6,7	164:15 169:18	269:5	70:25 71:5 72:25
36:20 101:15	<b>treating</b> 134:1	170:3 173:16	<b>Turow</b> 35:15,15	73:2 74:22,25 78:9
105:14 121:21	<b>treatment</b> 176:25	176:17 183:22	36:3 37:3 41:2,4	81:14 85:15 86:7,8
126:19 135:3	184:13	189:13 199:10	58:13 125:12	97:23 99:16
139:2 199:13	<b>tremendous</b> 316:7	219:22 220:15	<b>Turow's</b> 115:19	100:15,17 101:10
<b>traditionally</b> 101:17	<b>tremendously</b>	222:15 224:9	<b>TV</b> 130:11 179:13	124:21,24 125:1
223:25	155:15	231:11 232:10,14	179:14	190:2,10 201:10
<b>traffic</b> 24:25 250:13	<b>trend</b> 19:18 116:9	232:16 233:7	<b>TVs</b> 53:25	207:10 208:10
251:18 252:11,19	195:3,5,24 196:6	240:24 259:9	<b>tweak</b> 244:17	240:23 300:5
254:5 256:21,22	197:2	262:18 264:5	<b>tweet</b> 28:14	<b>types</b> 69:9 70:2,3,8
257:4,6	<b>trends</b> 6:6 52:5	265:19,19 266:2	<b>twice</b> 17:15 168:13	71:2,6 72:7,8,15
<b>train</b> 99:13,18	165:2 195:12,22	270:23 274:15	232:6,6	73:7,11,17 74:19
134:18 278:8	196:3	293:25 294:13	<b>Twitter</b> 22:20 23:6,6	75:18 77:10 80:21
280:5	<b>tricky</b> 305:7	301:23 316:24	263:11	82:25,25 83:2,4,15
<b>trained</b> 135:8	<b>tried</b> 14:17,20 53:14	<b>trying</b> 79:12,19	<b>two</b> 17:2 18:18	84:3,6 85:13 86:6
<b>training</b> 166:2,4	152:5 167:5	89:15 118:25	21:16 22:2,9,10	87:7 97:18,22
<b>trainings</b> 170:23	176:20 278:5	124:12 126:25	26:23 29:20 35:3	107:10 119:1
<b>trains</b> 99:12	290:19,22	145:10 149:15	37:6 43:22,22,23	191:10 204:8
<b>trait</b> 173:12	<b>tries</b> 167:24 263:25	155:7,19 161:12	48:8 52:2 63:18	210:22 213:19
<b>trajectories</b> 270:13	<b>trivial</b> 154:11	162:22 170:21	72:11 83:4,20	214:3 278:10
<b>transaction</b> 102:4	<b>trouble</b> 52:4 118:11	172:12 174:1,1	84:23,24 85:14	286:15 291:3
<b>transactions</b> 40:10	121:6 222:21	175:24 181:20	86:15 93:18 95:1	311:20
40:11 105:17	<b>troubles</b> 65:14	212:15 223:5	96:7,13 100:9	<b>typical</b> 212:20 218:1
<b>transcript</b> 318:6,7	<b>true</b> 56:7 61:17 76:6	227:7 230:16	110:6 115:13	219:2,12 308:7
318:20	123:23 137:18	238:22 241:14	131:15 137:2,11	<b>typically</b> 190:22
<b>transferred</b> 74:10	175:8 209:7	258:13,16 259:20	137:13 139:11,21	229:1 230:2,17
<b>transforming</b> 6:5	226:16 238:7	259:24 263:3,21	142:6 147:8	261:20 262:3
<b>translate</b> 51:15	246:3	266:4 277:22	148:17 149:4	263:9 284:11

<b>typing</b> 143:11	<b>understand</b> 11:22 30:1 35:25 40:2 41:9 44:9 49:1 50:24 59:12,13 69:13 70:8 81:7 98:10 99:21 112:21 113:19 121:3 123:13 132:18 133:3,6,16 138:20 164:24 165:4 172:22 189:6,14 197:14 199:11 207:15 209:10 218:20 223:5 224:9 225:9 225:10 227:8,9,10 229:13,17 231:11 232:11,14 233:7 237:16 239:12 261:13,14 263:3 273:8 297:16 314:21 315:14,25	<b>unfortunate</b> 298:19 <b>unfortunately</b> 128:3 128:10 161:1 213:8 <b>unhandled</b> 192:16 <b>unhappy</b> 12:14 <b>uniform</b> 97:10 <b>uninformed</b> 37:25 122:9 <b>uninstalling</b> 9:16 <b>unintelligibility</b> 311:3 <b>unintended</b> 133:25 160:16,21 183:3,3 <b>Union</b> 108:10 <b>unique</b> 6:21 27:17 29:9 78:8,9 100:20 152:2 156:21 158:2 228:17 268:8 <b>uniquely</b> 21:12 154:21 <b>unit</b> 10:24 302:13 308:3 <b>United</b> 1:1 98:25 108:9 189:3 <b>universally</b> 127:6,6 127:16,18 <b>universe</b> 71:6 <b>universities</b> 134:12 134:17 <b>University</b> 16:23 20:2,5 41:3 68:18 80:13 89:7,8 100:7 100:8 102:15 110:17 147:21 159:17 171:6 188:8,14 199:6 234:6 260:20 272:9 <b>unjust</b> 228:15 <b>unknowable</b> 56:2 <b>unknowingly</b> 85:22 <b>unknown</b> 56:10 <b>unknowns</b> 56:3 <b>unparalleled</b> 19:6 <b>Unpatched</b> 250:10	<b>unravel</b> 59:21 <b>unreasonable</b> 122:24 123:2 <b>unreasonableness</b> 122:23 <b>unregulated</b> 120:19 <b>unroll</b> 43:21 <b>unsolicited</b> 229:1,2 <b>unspecified</b> 132:16 <b>unsurprisingly</b> 52:16 238:20 <b>untangle</b> 274:15 <b>untargeted</b> 145:3 <b>untrained</b> 276:2,7 <b>untrusted</b> 264:16 <b>unusual</b> 218:22 <b>unwanted</b> 12:23 <b>unwarranted</b> 159:18 162:2,24 163:24 164:17 <b>update</b> 9:9 106:6 259:13 <b>updates</b> 256:17,22 <b>upload</b> 160:23 <b>uploaded</b> 254:17,24 <b>upset</b> 283:25 <b>upside</b> 211:8 212:17 212:19,19 213:17 <b>upswing</b> 15:22 <b>uptake</b> 102:21 <b>upward</b> 19:17 <b>urge</b> 57:6 146:7 <b>urged</b> 42:23 <b>URL</b> 269:10 <b>usability</b> 2:16 12:19 250:2,4 297:3,11 <b>usable</b> 82:6 272:4 282:15 297:14 <b>usableprivacy.org</b> 272:11 <b>usage</b> 19:18 75:8 127:9 216:18 221:13 <b>use</b> 4:6 8:17 15:22 16:10 17:16 20:20 20:23 21:12 23:2 28:23 29:17,23	30:19,24 32:7 41:14,21 42:11,24 43:5,6,6 45:15 48:21,23 55:12 57:16 64:1,16,18 64:20 65:10,12 66:1,21 67:6 72:18 74:9 76:25 78:8,20 80:3 85:5,22 86:2 92:13 96:24 97:2 97:18 98:3 99:22 106:5,8 107:20 108:8,23,25 109:2 111:24 112:12 118:22 120:25 121:20 125:4,5 131:8,11,20 132:1 132:10,13,17 133:4 134:5 143:22 149:15 151:20 155:1 156:6,7,15 164:15 166:3,9,20 167:10 170:9 172:25 181:20 185:18 199:10 207:14 209:14 210:8 214:6,14 215:1,20 224:24 242:2 251:1 264:1 267:23 273:2 278:8 279:14 287:17 302:22 308:7,8,9 316:6 <b>useful</b> 7:8 27:4 28:12 122:14 142:1 185:15 189:9 212:12 213:3 225:9 237:24 241:16 247:2 248:2 306:4 316:4,18 <b>user</b> 18:18 25:23 27:5 28:11 61:25 70:17 71:17,22 72:3,13,17 73:1,4 73:20,23 74:1 75:4
<b>typing</b> 143:11				
<b>U</b>				
<b>U.S</b> 33:20 49:20 214:13				
<b>Uber</b> 57:13 60:12,12 60:13				
<b>Ubi</b> 252:12 255:1,4 255:8,11				
<b>Ubi.com</b> 255:10				
<b>ubiquity</b> 106:24 111:12				
<b>UC</b> 171:7				
<b>ugly</b> 96:10				
<b>UI</b> 74:4				
<b>UK</b> 103:13 104:19 121:13				
<b>ultimately</b> 211:24 218:19 280:8				
<b>umbrella</b> 89:25				
<b>unacceptable</b> 12:10				
<b>unauthorized</b> 224:18,24				
<b>unaware</b> 70:11				
<b>unbalanced</b> 121:19				
<b>unclear</b> 85:10 111:21				
<b>uncomfortable</b> 92:24				
<b>unconcerned</b> 33:9 127:18				
<b>unconcerning</b> 127:6				
<b>unconsciously</b> 111:6				
<b>uncover</b> 173:13				
<b>undercurrent</b> 182:22				
<b>undercut</b> 183:14				
<b>underinvesting</b> 223:2 246:10				
<b>underlie</b> 97:11				
<b>underlying</b> 12:21 58:25 156:2 213:24 218:11 245:9 264:17				
<b>undermine</b> 56:7				
<b>underscores</b> 46:21				
<b>underserved</b> 8:23				

75:13,18,20 78:1 78:16 79:11 80:2,3 80:24 81:8,14,16 81:22 82:14 83:5,7 83:10,11,18,22,23 83:24 84:7,8,21 85:19,21,25 86:2,3 86:11 88:3,6,25 126:25 131:25 132:10 151:22 152:17 155:8 163:11,16,23 164:8,12 165:14 165:21 174:21 175:15 176:23 177:2 202:5,7,7,13 202:18 250:15 251:19,22 252:4 256:3 259:13 260:8,14,25 261:3 261:7 262:16 264:6 265:7,20 268:3,21,24 269:10,14 270:3 270:13,15,17 273:6 275:4 279:6 284:8 290:2 295:13 308:21 313:6 <b>user's</b> 28:10 79:3,14 79:23 253:24 261:6 269:16 270:10,15 <b>user-centric</b> 245:15 <b>user-facing</b> 308:19 <b>users</b> 16:12,13 17:13 17:22 18:7,16 19:11 20:19 21:18 21:25 22:20 23:9 23:18,19 26:1 27:5 32:4,4 61:3,8,23 69:7,12,17 76:23 77:2,19 78:9 79:21 79:22,23 81:4,7,9 81:10,17 82:24 83:14,15 86:12,19 86:20,23 87:3,9,22	88:16 89:1 118:25 139:8,11,15 140:15 141:4 143:13,14 144:3,3 144:9,19,19 145:1 145:4,8,9,13 150:13 161:3 163:17 165:23 169:1,1 175:1,9,11 175:12,15,22 176:15,17,22 194:10 237:12 259:5 261:17 262:12 263:23 264:1,13 265:23 270:23 272:17,23 273:9,10,14 274:11,18 275:5 280:22,23,24 281:1,4,11,16 282:7,10,12,16 284:9 286:4 288:11,24,25 289:4,6,22,23 290:6,20 291:7,21 293:14 294:9,11 295:20 308:14,15 308:17,18,20 310:24 311:8,10 311:18,19 312:11 313:4 315:14 <b>users'</b> 31:24 85:16 86:8,13,18 151:2,5 152:14 157:12 274:9 297:9,16 <b>uses</b> 45:17 46:14 65:21 67:5 112:16 127:9 148:5 150:6 150:11,12 157:15 202:14 299:14 <b>usually</b> 80:25 81:4 82:4,6,6 103:7 212:15 219:6 221:16 276:22 <b>utility</b> 86:3	<b>Vacation</b> 148:23,24 <b>vague</b> 276:17 277:21 <b>vagueness</b> 275:12 <b>vain</b> 310:22 <b>valid</b> 184:16 <b>validate</b> 166:10 <b>validated</b> 120:20 <b>validation</b> 208:22 209:5 <b>valuable</b> 7:7 157:3 174:13 215:13 <b>value</b> 12:5 37:18 39:4 42:10 43:13 120:22 207:19 246:24 256:4 312:11 <b>values</b> 205:9,10 238:3 <b>VANCE</b> 318:24 <b>variable</b> 92:9 93:6 94:18 95:16,16 98:8 153:14 193:19 <b>variables</b> 91:20,22 92:15 93:18 95:1 99:1 164:11 170:7 170:14 193:21 <b>variance</b> 79:5 <b>variation</b> 213:21,22 223:17 230:21 235:9 289:5 <b>varied</b> 83:21 234:2 <b>variety</b> 47:6 184:8 264:1 315:10 <b>various</b> 9:10 48:20 70:19 90:24 123:20 127:25 138:6,15 139:9,13 152:7 159:8 160:25 163:18,24 164:16 174:12 198:19 220:8 267:1 285:9 286:14,15 292:13 294:15 295:23 305:15	<b>vary</b> 81:13 83:23 111:7 <b>vast</b> 77:15 <b>vegetable</b> 39:11 <b>vehicle</b> 117:19 <b>vein</b> 32:10 <b>vendors</b> 304:15 <b>verbose</b> 285:17 <b>verbs</b> 33:10,11 <b>verify</b> 286:5 <b>Verizon</b> 19:12 <b>Veronica</b> 199:5,8 200:21 210:15 234:12 235:25 236:6 248:22 <b>versed</b> 310:5 <b>version</b> 210:9 289:6 290:9 300:22 <b>versions</b> 9:8,12,16 72:12 <b>versus</b> 83:6 88:8 89:13 90:22 103:20 113:25 118:14 189:25 193:2,13 201:3 207:11 232:4 285:10 286:25 287:4 <b>vertical</b> 203:14,19 204:12 206:22,25 208:2 <b>vexing</b> 9:23 <b>viable</b> 194:19 <b>vibrate</b> 71:20 <b>video</b> 20:15 99:14 229:2 265:1 <b>videos</b> 254:15 <b>view</b> 36:5 133:7 177:14 196:22 247:12,19 254:8 257:19 264:24 <b>viewed</b> 12:9 36:6 <b>viewing</b> 38:1 39:9 74:4,21 108:23 <b>views</b> 297:20 <b>violate</b> 64:8,9 134:2 <b>violates</b> 142:13	269:1 <b>violating</b> 22:24 <b>violation</b> 64:18 141:5 229:21 <b>violations</b> 146:5 224:8,23 225:2,7 228:24 229:10,16 229:18 231:10 <b>viral</b> 99:13 <b>virtually</b> 305:18 <b>virtuous</b> 133:17 <b>Visa</b> 232:20 <b>visibility</b> 78:15 143:21 145:15 150:8 <b>visible</b> 73:23 74:1 <b>vision</b> 284:25 292:5 295:14 296:13 312:20 <b>visit</b> 20:10 23:23 150:2 167:12 178:1 269:17 280:2 <b>visited</b> 16:25 17:2 17:13 137:15 141:15 151:22 178:2,10 269:8,10 269:14 <b>visiting</b> 17:16 18:15 20:11,12 23:24 25:2 29:25 61:9 <b>visual</b> 82:8,10,15 <b>visualization</b> 27:7 <b>visualized</b> 27:17 <b>Vitaly</b> 260:19,21 297:7 313:20 <b>vocal</b> 56:16 <b>voice</b> 9:24 255:6,7 <b>voicebox</b> 255:2 <b>voices</b> 42:18 <b>voluntary</b> 222:21 <b>vulnerabilities</b> 133:13 191:10,12 191:18,24 192:2,6 192:12,15,21 193:20 194:4,12 194:22 195:3,5,16
	<b>V</b>			

196:9,14,15,24 234:11 240:9 259:5,21 271:12 300:2,24 307:7 <b>vulnerability</b> 133:15 188:9,16 189:6,10 189:15,21 190:2,8 193:15 194:6 195:15 196:2,6 197:6 198:16 270:1 300:13 <b>vulnerable</b> 269:11	189:8 191:7 193:25 202:23 208:8,24 211:4 214:8 215:25 220:13 222:12,20 227:10 234:3,4 235:3 237:9 238:22 239:7 246:12 249:9 250:14 251:8 254:8 257:25 258:23 259:16 264:3,9,25 265:1,1 270:7 271:19 274:18,18,20 278:10,13 280:21 281:6,7 282:11,14 288:7,21 293:7 297:23 301:6 304:19 308:17 309:8,12,15 311:19 313:15 314:10 <b>wanted</b> 21:20 23:12 31:14 41:6 43:19 46:4,23 61:2 70:22 75:5 79:6 84:11 89:19,23 90:25 93:4 118:24 125:22 145:18 161:6 166:24 169:22 170:1 176:3 180:21 184:24 185:1 231:14 232:10,18 245:7 246:22 248:23 271:9 303:14,15 312:15 313:21,23 314:4 316:13 <b>wants</b> 185:18 <b>warned</b> 293:19 <b>warrant</b> 116:9 <b>wary</b> 132:5 <b>Washington</b> 1:11 32:4 <b>wasn't</b> 23:6 75:21	94:17 183:7 <b>waste</b> 179:9 <b>watchdogs</b> 151:4 <b>watching</b> 4:12 179:14 <b>water</b> 4:7 128:16 <b>way</b> 7:4,15 14:11 22:22 24:20 27:14 34:2 35:13 42:11 43:23 44:1 49:5 51:8 55:12 60:10 64:11 77:12 98:18 99:22,25 101:2 103:16,25 104:5 110:8 114:22 128:19,24 134:22 140:1 143:19 154:21 161:13 163:9 165:9 171:2 173:14 174:5,21 176:16,17,20 179:17 182:2 185:21 199:19 203:17 213:23 214:21 215:6 216:11 222:23 227:8 238:17 245:23,24 246:4 258:10,24 260:25 262:1,9 264:16 265:10,23 268:20 269:1,20 272:25 274:7 280:17,19 281:11 286:5,22 287:16,21 288:5 289:19 290:24 292:2 294:5,8,21 296:1 298:13 300:14 304:13,21 307:1,25 309:13 310:10,14 311:21 316:21 <b>ways</b> 31:21 40:13 41:20 43:7 75:14 99:12,17 134:1 139:13 176:9 214:23 224:15	227:12 236:12 238:10,25 263:19 274:22 282:11 295:15 297:16 310:25 314:24,25 315:7 <b>we'll</b> 11:16,18 12:16 65:8 89:6 110:14 116:5 142:6 153:8 164:22 165:25 166:9 185:9 225:1 296:25 <b>we're</b> 4:2 5:1 11:5 15:9 20:1,8 21:1 24:9 25:2,13 26:10 26:10,11,15 31:11 33:7 34:12 51:11 51:25 53:25 54:10 60:6,7 64:19 67:12 68:3 77:21 78:11 78:24 79:12,16 91:13 92:16 93:3 95:12 99:18 100:14,22,23 103:20 110:19 113:20 114:17 115:5 117:11 120:12 126:5,6 130:3 134:10 136:9,13,23 147:20 162:21 164:15 170:18,21 172:4 173:4,15 176:5 179:20,22 181:1,5,6,7,23 212:11 213:18 214:4,25 215:1,16 215:19 216:1,3,4,4 216:13 218:1,19 220:19 223:9 229:7,20,20,23 231:10 256:11 258:16 277:22 279:20,25 281:14 281:17 282:6 288:10,12,13 291:14 293:8,22	293:23 299:24 301:10 303:14 307:3,7,13,13 309:24 311:6,10 313:16,18 316:18 <b>we've</b> 7:15,22 23:16 53:18 62:16 68:23 76:24 93:13 95:5 102:15,17 103:2 103:13 118:14 126:7,24 128:4 151:7 152:4 157:6 159:22 163:2 171:8,22 175:22 185:22 186:5 214:13,23 220:21 258:25 259:17,19 278:5,5 280:10 283:8 288:18 291:2 299:12 301:14 308:24 311:8 <b>weakness</b> 64:2 <b>weaknesses</b> 248:8 <b>wearable</b> 127:13 <b>web</b> 15:12,24 16:7 16:22 17:10 19:13 19:16,20 20:2,6,9 20:25 21:5 22:17 25:5 26:2,7 29:14 30:2,23 31:5,21 53:23 125:14 137:9,13,15 138:14 141:17 148:5 149:11,24 149:25 150:9,23 150:25 170:13 171:11 174:25 188:8 189:8 191:2 196:16,22 197:16 246:16 254:13 261:19,19,20,21 261:23 264:7,9,13 269:7 271:2,2 284:22,23 294:24 <b>web's</b> 148:2 <b>webcast</b> 4:11,13,13
--	---	--	---	--

208:24	126:25	<b>Whittington</b> 40:16	<b>Wooyun</b> 188:24	283:13 284:21,22
<b>WebRTC</b> 26:3,25	<b>weight</b> 40:23	<b>wide</b> 7:19	189:1 190:5,18	284:23 288:8
28:6,6,20	<b>weird</b> 95:4 96:10	<b>widely</b> 33:16	191:9 192:2,8	291:3 292:4
<b>website</b> 24:23,24	265:9 266:1	<b>widespread</b> 41:13	195:21 196:7	293:24 305:24
27:14 35:21 52:20	273:11	49:20 50:7 142:12	197:2	<b>worked</b> 21:21 27:12
80:21 81:2,14	<b>welcome</b> 3:3 4:12	147:10 184:3	<b>word</b> 42:25 65:12	99:20 130:17
82:17 83:6,7,17,21	5:18 30:21 136:4	185:16	135:5	309:20
83:24 84:8,9,13,15	149:24 188:3,10	<b>WiFi</b> 45:15 76:16	<b>wording</b> 108:8	<b>worker</b> 117:7
85:2,8,17,19,22,24	250:5 297:23	292:19,21	<b>words</b> 102:24	<b>working</b> 75:15 77:1
86:1,3,6,7,20	310:18 313:23	<b>wild</b> 73:10 302:16	104:12	112:21 121:16
87:15 106:5,12	<b>welcomed</b> 196:22	<b>willfully</b> 64:8,8	<b>work</b> 6:10 7:9,16	138:12 143:5
108:24,25 109:2	<b>welfare</b> 199:14	<b>willing</b> 12:4,11	9:2 10:20,24 11:2	147:15 163:7
118:22 120:12,14	201:2	42:13 181:16	11:3 13:20 20:7	165:17 172:8
141:15,20 163:19	<b>well-defined</b> 168:10	202:12 284:16	22:10,13,15 25:25	173:18,23 175:19
178:1,12 190:2	<b>well-developed</b>	289:16	32:2 35:10,11,11	176:14 208:21
195:7 247:23	197:8	<b>willingness</b> 42:9	36:9 38:22,23 39:5	215:8 280:10
249:8 269:18	<b>well-known</b> 154:18	111:5	39:6,7 40:7 52:9	300:21 309:7
272:11 280:2	156:16 169:6,11	<b>win</b> 100:9	53:1,5 57:23 59:23	<b>works</b> 8:11 24:16
281:12	<b>went</b> 21:19 47:11	<b>win-win</b> 200:11	68:13,22 69:1	27:14 138:17
<b>website's</b> 80:25	48:1 53:7 116:2	201:3	76:24 77:21 79:4,9	139:6 152:10
<b>website-specific</b>	125:7 217:8	<b>window</b> 138:16	88:18 94:3 96:6	153:24 157:13
87:8	232:13 252:7	<b>winner</b> 202:16	99:21 100:10	165:6,9 184:5
<b>websites</b> 16:1,3,4,21	<b>weren't</b> 14:14 48:9	203:25	106:3 110:6,21	201:19 202:4
17:1,3,8,14,16,17	56:5 182:14	<b>winning</b> 10:14	113:1,12 115:20	233:4 240:3 251:5
17:18,18,19 18:16	256:17	167:15	121:23 122:11,17	261:14,17 262:2
18:22 19:3,4,9,9	<b>West</b> 225:17	<b>wins</b> 202:15	134:24 138:23	264:20 270:11
21:13 31:21 71:13	<b>Westin</b> 33:10,21	<b>wireless</b> 45:5,15	145:23,24,25	<b>workshop</b> 1:4 8:8,11
80:19,20 81:9,11	34:1,10 35:9 38:21	<b>Wireshark</b> 253:10	146:9,10,13,25	14:8 53:25 300:7
81:12,17,18 83:9	38:22 39:2 60:5	<b>wish</b> 14:19 114:23	148:3 152:12	317:7 318:3
83:15,16 84:18	<b>Westin's</b> 31:12 33:1	179:10 201:21,24	161:9,16 162:3,9	<b>workshops</b> 7:22 8:2
86:14,18,24,25	34:19 35:6 36:5	236:1 237:1,18	166:17 172:3,4	299:20
87:4,5,9,10,12,13	37:23	239:8 244:13	173:24 174:13,13	<b>world</b> 8:7 10:4 40:7
87:22,23 88:22	<b>what's</b> 62:3	<b>wishes</b> 190:7	174:25 176:10	40:9 49:1,15 50:22
90:24 118:21	<b>wheels</b> 131:24	<b>wishful</b> 243:23	180:13,17 182:15	51:10 56:2 58:14
119:2 139:9	<b>white</b> 42:18 188:17	<b>Wizard</b> 58:18	185:16 186:12	172:15 173:22
140:18 147:4,6	<b>white-hat</b> 191:16	<b>woman</b> 178:22,22	188:12 199:8,9,17	174:18 193:8
151:22 152:6,7	192:1 194:3,11,23	<b>women</b> 91:10,16	201:14 208:25	212:1 245:17,19
178:3,6,10 191:23	196:7,25 247:18	140:24 169:16,24	210:5,6,23 212:16	293:20
192:13 194:8	248:5,16	177:17 178:16	212:23 222:11,14	<b>worlds</b> 6:24
198:2,18,23	<b>white-hat-initiated</b>	179:3,20 180:3,8	223:5,14 229:6	<b>worldwide</b> 63:18
201:21 272:18	191:1 192:1,24	181:15,16,17	236:16,22,24,25	<b>worried</b> 67:1 173:6
274:3 281:9,10	198:8,11	182:5 186:5	237:2,3,18 238:1	217:5 221:5
<b>week</b> 5:2 8:15 74:10	<b>white-hats</b> 189:14	<b>wonder</b> 300:9	238:15,21 239:10	<b>worry</b> 213:21 217:3
74:13,16 133:22	189:20 191:22	<b>wonderful</b> 130:20	240:5,18 250:10	218:2
<b>weekend</b> 53:7	193:23 194:13	225:14,18 234:2	259:1,3,16 263:3	<b>worrying</b> 121:12
<b>Weeyun</b> 189:25	197:20,22 198:12	238:17 314:5	271:9 273:16	<b>worst</b> 37:11
<b>weigh</b> 33:4,14 50:8	240:1,11	<b>wondering</b> 125:25	275:6,10 283:11	<b>worth</b> 39:1 247:14

<b>wouldn't</b> 35:4 121:8 151:16 164:1 176:6	19:17 21:16 22:9 31:20 35:16 37:2 43:22,22 56:3 63:19 69:15 72:11 102:16,17 116:14 116:14 127:7 135:18 151:7 215:2 222:15 223:12,25 226:14 226:25 228:22 229:6 230:16 236:16,23,24 240:22 245:21 283:3 288:2 307:19	<b>1,700</b> 228:6 <b>1/20/16</b> 318:12 <b>1:00</b> 128:25 <b>1:12</b> 130:2 <b>10</b> 91:10 103:16 186:2,23 236:23 257:12 276:2 277:7 278:11 290:18 <b>10-minute</b> 67:18 <b>10-year</b> 91:17 <b>10,000</b> 63:18 <b>100</b> 16:21 17:14,18 18:21 19:3,9 190:17 194:2 279:21 282:2 284:10 <b>100,000</b> 144:10 <b>11</b> 87:25 88:2 <b>12</b> 14:16 <b>12,000</b> 224:6 <b>12:20</b> 129:3 <b>121</b> 29:8 <b>130</b> 2:5 <b>136</b> 2:13 <b>14</b> 1:6 2:10 318:4 <b>15</b> 14:22 54:13 <b>15-minute</b> 68:11 <b>150</b> 284:15,16 <b>16</b> 84:18 <b>17</b> 83:25 87:19,20 88:1 <b>188</b> 2:15 <b>19</b> 14:18 47:15 <b>192.168.1.2</b> 28:12 <b>1970s</b> 39:20 236:13 <b>1975</b> 169:20 <b>1980s</b> 38:14 236:14 <b>1995</b> 188:18 <b>1997</b> 15:25 <b>1999</b> 15:18	125:15 157:25 194:15 218:25 248:19 307:19 <b>20-minute</b> 45:2 <b>20,000</b> 148:17 158:1 <b>200</b> 17:19 77:8 <b>200,000</b> 231:3,5 232:11 235:1 <b>2000</b> 213:20 <b>2009</b> 37:6 <b>200K</b> 144:13 178:13 <b>2010</b> 62:23 189:1 213:20 <b>2011</b> 16:3,5 <b>2012</b> 16:7 17:15 18:22 21:14 37:14 <b>2013</b> 189:4 <b>2014</b> 21:4,19 <b>2015</b> 16:8 18:22 45:3 <b>2016</b> 1:6 318:4 <b>21</b> 46:2 <b>23</b> 15:25 <b>23andMe</b> 211:18 <b>24</b> 17:17 29:9 69:22 <b>240</b> 84:18 <b>240,000</b> 288:24 <b>25</b> 130:19 192:14 212:23 <b>25,000</b> 16:21 63:17 <b>250</b> 2:16 <b>26</b> 91:11 276:11 <b>27</b> 75:9 77:6 <b>270</b> 230:23 <b>275</b> 18:17 <b>28th</b> 280:2	<b>300</b> 17:20 69:16 148:14 228:7 <b>314</b> 2:6 <b>32</b> 49:10 <b>33</b> 47:11 <b>33-day</b> 157:24 <b>35</b> 88:2 <b>35.9</b> 91:17 <b>36</b> 73:14 75:6,8 79:4 104:20 <b>360-degree</b> 43:17 <b>360,000</b> 10:17 <b>39</b> 109:5
<hr/> <b>X</b> <hr/>	<hr/> <b>Z</b> <hr/>	<hr/> <b>3</b> <hr/>	<hr/> <b>4</b> <hr/>	
<b>X</b> 2:1 79:19 127:9 <b>X-axis</b> 205:5	<b>yellow</b> 206:1,9 207:6 <b>yes/no</b> 85:14,17 86:18 88:7,8,12 <b>Yeung</b> 3:3,4 <b>yield</b> 74:5 153:19 154:8 <b>yields</b> 247:1 <b>yippy</b> 57:15 <b>York</b> 20:10 29:7,7 223:22 <b>you'd</b> 124:8 <b>younger</b> 93:12,14 <b>YouPorn</b> 23:11,13 <b>YouTube</b> 20:14 99:15 152:7	<b>2</b> <hr/>	<b>4</b> 2:14 188:1,5 232:4 <b>40</b> 46:17 73:13 104:20 111:19 231:21 236:16 <b>400</b> 1:10 <b>43</b> 46:11,15 47:20 104:19 <b>44</b> 191:11 <b>443</b> 256:14 <b>45</b> 144:10 190:7 312:14 <b>47</b> 104:15	
<hr/> <b>Y</b> <hr/>	<hr/> <b>0</b> <hr/>	<hr/> <b>3</b> <hr/>	<hr/> <b>5</b> <hr/>	
<b>Y-axis</b> 205:7 <b>Yahoo</b> 42:8 43:13 160:3 <b>yeah</b> 53:12,13 59:3 66:13 80:15 88:17 89:3 109:9 122:21 159:4 174:15 245:18 248:22,23 <b>year</b> 10:21 60:8 102:22 116:14 127:11 167:13,20 168:13 215:23 216:4 280:1 282:3 317:4 <b>years</b> 16:2 17:25	<b>Z-Wave</b> 257:18 <b>Zeide</b> 15:6 54:22 65:9,19 <b>Zhang</b> 199:8 <b>Zhao</b> 188:12 <b>ZigBee</b> 257:18 <b>zoomed</b> 289:2	<b>2</b> 2:11 68:1 153:17 <b>20</b> 21:17 25:17 47:21 68:12 91:10 102:16 110:14	<b>5</b> 2:4,16 230:17 231:12 250:1 300:13 <b>5,600</b> 224:5 <b>5.2</b> 232:24 <b>5.6</b> 291:12 <b>5.9</b> 232:24 <b>5:43</b> 317:7 <b>50</b> 78:11 186:1 196:1 232:1 284:10 <b>51</b> 50:2 <b>548</b> 19:9 <b>55</b> 45:19 <b>57</b> 19:8 49:8 <b>58</b> 48:13	
	<hr/> <b>1</b> <hr/>	<hr/> <b>3</b> <hr/>	<hr/> <b>6</b> <hr/>	

---

**6,000** 17:14 75:7**60** 10:17 75:19**68** 2:12

---

**7**

---

**7** 230:18 231:12**70** 88:12 213:14**70s** 169:12 236:18**71** 45:16 107:6**74** 18:22**75** 37:6 75:16

111:17 288:15

**750** 45:4**756** 45:5**7th** 3:22

---

**8**

---

**80** 141:5 228:16,17

257:6 277:6

**80s** 236:18**83** 18:14**84.7** 18:24**85** 78:19,24 167:19

288:15

**871** 91:15

---

**9**

---

**9** 232:3**90** 14:15 103:19**91** 45:12**92** 18:22 19:3

289:16

**923** 19:4**93.5** 18:24**95** 22:4 152:11

229:11 283:23

289:18