

In the Matter of:
Informational Injury Workshop

December 12, 2017

Condensed Transcript with Word Index



For The Record, Inc.
(301) 870-8025 - www.ftrinc.net - (800) 921-5555

1

1 UNITED STATES FEDERAL TRADE COMMISSION
 2 BUREAU OF CONSUMER PROTECTION
 3 BUREAU OF ECONOMICS
 4
 5
 6 INFORMATIONAL INJURY WORKSHOP
 7
 8
 9 TUESDAY, DECEMBER 12, 2017
 10 9:15 A.M.
 11
 12
 13 CONSTITUTION CENTER CONFERENCE CENTER
 14 400-7TH STREET, S.W.
 15 WASHINGTON, D.C. 20024
 16
 17
 18
 19
 20
 21
 22
 23
 24
 25 Reported by: Susanne Bergling, RMR-CRR-CLR-CMRS

2

1 C O N T E N T S
 2
 3 INTRODUCTORY REMARKS: Page 3
 4 Cora Han
 5
 6 OPENING REMARKS: Page 6
 7 Acting Chairman Ohlhausen
 8
 9 PANEL 1: INJURIES 101 Page 15
 10
 11 PANEL 2: POTENTIAL FACTORS IN Page 68
 12 ASSESSING INJURY
 13
 14 PANEL 3: BUSINESS AND CONSUMER Page 141
 15 PERSPECTIVES
 16
 17 PANEL 4: MEASURING INJURY Page 208
 18
 19 CLOSING REMARKS Page 270
 20 Andrew Stivers
 21
 22
 23
 24
 25

3

1 P R O C E E D I N G S
 2 - - - - -
 3 (Proceeding called to order, 9:15 a.m.)
 4 INTRODUCTORY REMARKS
 5 MS. HAN: Good morning. Welcome. On behalf of
 6 my colleagues here at the Federal Trade Commission, I'm
 7 happy to welcome you here to our Informational Injury
 8 Workshop. We are happy to see so many of you here
 9 today.
 10 My name is Cora Han, and I'm an attorney in the
 11 Division of Privacy and Identity Protection here at the
 12 Commission. My co-organizers for today's event are
 13 Jacqueline Connor, also from the Division of Privacy and
 14 Identity Protection, and two colleagues from the Bureau
 15 of Economics, Doug Smith and Dan Wood.
 16 Before we get started with our program, I need to
 17 review a few administrative details. Please silence any
 18 mobile phones and devices. If you must use them during
 19 the workshop, please be respectful of the speakers and
 20 your fellow audience members.
 21 Please be aware that if you leave the
 22 Constitution Center Building for any reason during the
 23 workshop, you will have to go back through security.
 24 Please bear this in mind and plan ahead, especially if
 25 you are participating in a panel, so we can do our best

4

1 to remain on schedule.
 2 The restrooms are right outside the auditorium.
 3 The Plaza East Cafeteria is located inside the building,
 4 so you can use it without going through security again.
 5 The cafeteria is the place to go if you want coffee
 6 without having to leave the building. It will be open
 7 during the first part of our midmorning break until
 8 11:00, and then after it will reopen at 11:30 and remain
 9 open until 3:00. Please remember, however, that no food
 10 or drink, other than water, is permitted in the
 11 auditorium.
 12 Most of you received a lanyard with a plastic FTC
 13 event security badge. We reuse these for multiple
 14 events, so when you leave for the day, please return
 15 your badge to FTC event staff.
 16 If an emergency occurs that requires you to leave
 17 this conference room but remain in the building, follow
 18 the instructions provided over the building PA system.
 19 If an emergency occurs that requires the evacuation of
 20 the building, an alarm will sound. Everyone should
 21 leave the building in an orderly manner through the main
 22 7th Street exit. After leaving the building, turn left
 23 and proceed down 7th Street and across E Street to the
 24 FTC emergency assembly area. Remain there until
 25 instructed to return to the building. If you notice any

5

1 suspicious activity, please alert building security.
 2 Please be advised that this event may be
 3 photographed, and it is being webcast and recorded. It
 4 is also being broadcast via Facebook Live. By
 5 participating in this event, you are agreeing that your
 6 image and anything you say or submit may be posted
 7 indefinitely at ftc.gov or on one of the Commission's
 8 publicly available social media sites.
 9 We're happy to welcome those watching via the
 10 webcast. We will make the webcast and all of the
 11 workshop materials available online to create a lasting
 12 record for everyone interested in these issues.
 13 There will be time for audience questions during
 14 each of the panels today. Question cards are available
 15 on the table in the hallway immediately outside of the
 16 auditorium and also from FTC staff inside the
 17 auditorium. If you have a question, please fill out a
 18 card, raise your hand, and someone will come and get it.
 19 Please understand that we may not be able to get to all
 20 audience questions, but we will do our best.
 21 For those of you on Twitter, we will be tweeting
 22 today's workshop at #infoinjuryftc, and if you would
 23 like to ask a question via Twitter, please tweet your
 24 question using that hashtag.
 25 Lastly, I want to say thank you to our panelists

6

1 for taking part today. We are grateful for your time
 2 and work in the privacy and security area. Aside from
 3 the folks that you will see on stage today, this program
 4 would not be possible without the great work done by
 5 Kristal Peters and Bruce Jennings, alongside our
 6 paralegal support today from Carrie Davis, Anne
 7 Blackman, Olivia Berry, Courtney Brown, Christine
 8 Barker, Amber Howe, and Aaron Kaufman.
 9 Also providing invaluable support are Nathan
 10 Otlewski from our Division of Consumer and Business
 11 Education and Nicole Jones and Juliana Henderson from
 12 our Office of Public Affairs. Thank you, all.
 13 Now, it is my honor to welcome our Acting
 14 Chairman, Maureen Ohlhausen, to give opening remarks.
 15 (Applause.)
 16 **OPENING REMARKS**
 17 **ACTING CHAIRMAN OHLHAUSEN:** Well, good morning,
 18 everyone, and thank you for being here for today's
 19 workshop on information injury. I'd also like to thank
 20 all the staff who have worked so hard to make this
 21 workshop possible. Special thanks to Doug Smith and Dan
 22 Wood from the Bureau of Economics and Cora Han and
 23 Jacqueline Connor from the Bureau of Consumer
 24 Protection. The four of you exemplify the interbureau,
 25 cross-disciplinary collaboration that is a unique

7

1 strength of the FTC and that is particularly important
 2 for complex topics like informational injury.
 3 So to start with the fundamentals, information
 4 injury is my term for the harms consumers may suffer
 5 from privacy and data security incidents. In a speech
 6 in September on painting the privacy landscape at the
 7 FTC, I described some of the types of injury to
 8 consumers that the FTC has encountered in its privacy
 9 and data security cases over the years. I also
 10 announced my three goals for this workshop.
 11 First, better identify the qualitatively
 12 different types of injury to consumers and businesses
 13 from privacy and data security incidents. Second,
 14 explore frameworks for how we might approach
 15 quantitatively measuring such injuries and estimate the
 16 risk of their occurrence. And third, better understand
 17 how consumers and businesses weigh these injuries and
 18 risks when evaluating the trade-offs to sharing,
 19 collecting, storing, and using information.
 20 My ultimate goal is to use what we learn today to
 21 guide FTC case selection and policy work going forward.
 22 Our discussions will explore the types of negative
 23 outcomes that arise from the unauthorized access or
 24 misuse of consumer data and consider factors in
 25 assessing consumers' informational injury. We will also

8

1 examine business and consumer perspectives on the
 2 benefits, costs, and risks of collecting and sharing
 3 consumer information. And, finally, we will grapple
 4 with how to measure informational injuries.
 5 But before we get to these important discussions,
 6 I would like to touch briefly on the FTC's role in
 7 privacy and data security and talk about why this
 8 workshop is both timely and important. Now, as I never
 9 tire of saying, the FTC is the primary U.S. enforcer of
 10 commercial privacy and data security obligations. We
 11 take that charge very seriously. We have brought more
 12 than 500 privacy- and data security-related cases, both
 13 online and off, and under my leadership, this work has
 14 continued. Since this summer, we have announced six
 15 important privacy or data security cases, Uber,
 16 TaxSlayer, Lenovo, and three cases enforcing obligations
 17 under the EU-US Privacy Shield Agreement.
 18 Our primary privacy and data security tool is
 19 case-by-case enforcement under Section 5 of the FTC Act
 20 to protect consumers from deceptive or unfair acts or
 21 practices. One significant benefit of this approach is
 22 that it limits the need for policy makers to predict
 23 future developments in the marketplace. This is
 24 especially important in complex, fast-changing
 25 technology industries and in areas such as privacy,

9

1 where consumers have a wide range of evolving
 2 expectations and preferences.
 3 Case-by-case enforcement focuses on real world
 4 facts and specifically alleged behaviors and injuries.
 5 Each case integrates feedback on earlier cases from
 6 consumers, industry advocates, and, importantly, the
 7 courts. This ongoing process recognizes that markets,
 8 consumer expectations, and consumer benefits and risks
 9 evolve with new technologies, and it protects consumers
 10 while allowing innovation to occur.
 11 In addition to Section 5, we enforce rules under
 12 specific statutes, such as the Gramm-Leach-Bliley Act
 13 and the Children's Online Privacy Protect Act, and we
 14 offer copious amounts of consumer and business education
 15 on these topics.
 16 Now, given the FTC's past record, you may ask,
 17 why hold a workshop on informational injury now? I've
 18 chosen to focus on consumer informational injury for two
 19 key reasons. First, in making policy determination,
 20 injury matters. Although the free market is a powerful
 21 institution for improving human welfare, consumers can
 22 and do suffer injury from some business practices.
 23 Government does the most good with the fewest unintended
 24 side effects when it focuses on addressing actual or
 25 likely substantial consumer injury instead of expending

10

1 resources to prevent trivial or purely hypothetical
 2 injuries. We need to understand consumer injury to
 3 weigh effectively the benefits of intervention against
 4 its inevitable costs.
 5 Tom Leonard, in his comment for the Technology
 6 Policy Institute, argued this point quite nicely, noting
 7 that privacy benefits us because it reduces harms from
 8 information misuse, but if there are no harms, then data
 9 use restrictions impose only costs and no benefits.
 10 Policymakers and enforcers, therefore, need to
 11 understand how and how much consumers are injured by
 12 various practices involving the collection, use, and
 13 disclosure of consumers' information. More precisely,
 14 we need a framework for principled and consistent
 15 analysis of consumer injury in the context of specific
 16 privacy and data security incidents.
 17 The FTC's deception and unfairness statements
 18 provide such frameworks for thinking about consumer
 19 injury generally, but it's worth exploring more deeply
 20 how those frameworks apply in the specific setting of
 21 privacy and data security.
 22 Now, speaking of unfairness, the second reason
 23 I've chosen to focus on consumer injury is because it is
 24 a key part of our Section 5 unfairness standard. The
 25 focus of our discussion today is on defining consumer

11

1 informational injury as a descriptive and economic
 2 matter, but I hope that what we learn today can help
 3 guide the future application of the unfairness
 4 standard's substantial injury prong.
 5 As for why hold the workshop now, as I've
 6 mentioned, the FTC has been a very active privacy and
 7 data security enforcer, and many of our cases
 8 appropriately focus on the most egregious low-hanging
 9 fruits where the harms were obvious to the affected
 10 consumers, the FTC, and often the defendants.
 11 For example, we have a series of cases, such as
 12 LeapLab, Sequoia One, and the recent Blue Global case,
 13 that involve data providers who sold sensitive credit
 14 and payment information when they knew or should have
 15 known that the buying party was a fraudster who was
 16 going to misuse that information.
 17 There were other types of cases involving direct
 18 financial loss for consumers. For example, the Wyndham
 19 data breaches allegedly resulted in identity theft and
 20 fraudulent charges to consumers. In the recent
 21 TaxSlayer case, the breached tax return information
 22 allegedly resulted in fraudulent tax filings, delaying
 23 consumers' receipt of their tax refunds.
 24 But as technology and business models continue to
 25 evolve, we have and are likely to continue to face more

12

1 challenging scenarios that involve harms other than
 2 financial loss. For example, we took action against
 3 Accusearch for selling illegally obtained personal
 4 telephone records of individuals, where we had evidence
 5 that stalkers and abusive former spouses used this
 6 information to surveil and harass individuals. We also
 7 brought a case against the operator of a revenge porn
 8 website whose posting of highly sensitive intimate
 9 photos and personal information generated threats to and
 10 harassment of victims. And consider also the news
 11 reports of at least one suicide associated with the data
 12 breach at infidelity-promoting website Ashley Madison.
 13 A strong framework for assessing consumer injury
 14 in such cases will serve two purposes. First, it will
 15 help us think critically as we monitor new technologies
 16 and data uses for potential consumer injury. Second, it
 17 will help establish criteria by which we can judge if
 18 privacy and data security enforcement is the proper tool
 19 to address a practice or if other mechanisms, perhaps
 20 either other agencies, institutions, or laws, would be
 21 better equipped to address any particular negative
 22 outcome.
 23 I believe our discussion today will help ensure
 24 we have such a framework. First, we need to examine
 25 more thoroughly the range of injuries that can occur

1 from privacy and data security incidents. We are
2 generally familiar with the direct financial injuries
3 from identity theft, for example. We have also seen
4 examples of unwarranted health and safety risks and
5 intrusion into seclusion, and our first panel today will
6 talk about the different kinds of injury suffered by
7 consumers because of privacy incidents and data security
8 breaches.

9 Second, we need to understand the key factors
10 that matter in assessing injury from privacy and data
11 security violations. Some obvious ones are the type of
12 data involved, the magnitude of harm, and the
13 distribution of the injury. But what else? And are the
14 same factors relevant in both the privacy and data
15 security context? What is the relationship between risk
16 and injury? Finally, when is FTC intervention
17 appropriate? Our second panel will tackle these issues.

18 Third, we can benefit from learning about how
19 companies weigh the potential benefits and costs of
20 collecting and using information and how this affects
21 the decisions they make about protecting or restricting
22 such information. Similarly, how do consumers weigh the
23 benefits and costs of sharing information? And our
24 third panel will dig into those issues.

25 Finally, we seek a better understanding of how to

1 quantify consumer informational injury. Now, there's an
2 old saying often attributed to management expert Peter
3 Drucker. "What gets measured gets managed." If we want
4 to manage privacy and data security injuries, we need to
5 be able to measure them. Our fourth panel will discuss
6 the challenges of quantifying informational injury and
7 how we can tackle those challenges.

8 At the end of the day, Andrew Stivers, Deputy
9 Director of our Bureau of Economics, who has already
10 done valuable work on these issues, will provide some
11 closing remarks. This workshop is the next step in an
12 ongoing conversation about consumer informational injury
13 and how we can address it effectively, both here at the
14 FTC and in the marketplace. This is going to be a
15 fascinating discussion, and I again thank all of you for
16 joining us, and I look forward to starting the first
17 panel. So thank you very much.

18 (Applause.)
19
20
21
22
23
24
25

PANEL 1: INJURIES 101

1 MR. WOOD: Okay. To start off today's workshop,
2 we will be exploring the broad array of negative
3 outcomes that result from unauthorized access or misuse
4 of consumers' personal information. We are fortunate to
5 have a panel of experts today who can speak to a wide
6 and varied range of injuries. We hope that this first
7 conversation will provide concrete examples that later
8 panels can draw from while discussing various aspects of
9 informational injury.

10 We're planning to devote -- so we have five
11 wonderful panelists that we are very happy can join us,
12 and we will spend the majority of the panel hearing from
13 them. We are planning to devote the last ten minutes to
14 audience questions. So if you would like to ask a
15 question, you need to find a question card. They are
16 outside the auditorium or you can also raise your hand
17 and I believe paralegals have them. Then you pass the
18 question card to a paralegal, and they will bring it up
19 here.

20 So with that, let me introduce the panelists. So
21 Pamela Dixon is the founder and executive director of
22 the World Privacy Forum, a public interest research
23 group known and respected for consumer and data privacy
24 research.
25

1 David McCoy is an assistant professor in the
2 Computer Science Department at NYU Tandon School of
3 Engineering. His research interests are in the areas of
4 security, privacy, and empirical measurement. Some of
5 his current interests span from the socioeconomics of
6 cyber crime to automotive computer systems.

7 Lauren Smith is policy counsel at the Future of
8 Privacy Forum where she focused on big data, the
9 internet of things as related to connected cars, data
10 ethics, algorithmic decision-making, and drones.

11 Cindy Southworth is the executive vice president
12 of the National Network to End Domestic Violence. She
13 founded the Safety Net Project which focuses on the
14 intersection of technology and intimate partner abuse.

15 Finally, Heather Wydra is a supervising attorney
16 at Whitman-Walker Health's Legal Services Program. Her
17 practice areas include discrimination in employment by
18 places of public accommodation and in healthcare, as
19 well as representing clients who have been denied access
20 to health insurance coverage or disability benefits.

21 Now that we have those quick introductions done,
22 let's get this panel and the workshop itself started by
23 discussing the various types of informational injuries
24 and consumer harm that our panelists have seen.

25 MS. CONNOR: Thanks, Dan.

17

1 My name is Jacqueline Connor, and I'm an attorney
 2 with the Division of Privacy and Identity Protection,
 3 and so today we are going to start the panel off by
 4 asking each panelist one question and kind of giving
 5 them some time to answer, and then we will jump into a
 6 more general group discussion when the panelists can
 7 jump in whenever they want to.
 8 So, Pam, we are going to start with you, and you
 9 have the clicker for the slides. Unfortunately, today,
 10 identity theft as a term has been part of our lexicon,
 11 and the harm to consumers goes beyond what we consider
 12 traditional identity theft. Can you describe some of
 13 those other different types of identity theft?
 14 MS. DIXON: First, thank you for the invitation
 15 to share my research and knowledge today, and I am
 16 really grateful that the FTC is holding this workshop.
 17 I think it's good timing and a good topic, so thank you.
 18 So I think everyone is familiar with various
 19 financial forms of identity theft. We have probably all
 20 experienced an incident where we get a phone call from
 21 our financial services company, and they say, oh, by the
 22 way, we are going to issue you a new card because, you
 23 know, someone is using your card.
 24 So that's a lot different, that annoyance is a
 25 lot different, than, for example, the woman I met and

18

1 worked with who was from Utah, who had her children
 2 taken away from her through the actions of a medical
 3 identity thief. In her particular situation, what
 4 happened is that an imposter had taken her identity
 5 information, just gleaned from a simple phone book call,
 6 and this woman went around to emergency rooms around
 7 Utah seeking painkiller drugs. And the police came, and
 8 when they arrested this person who was a problem, they
 9 came to the victim's house, arrested her, and took her
 10 kids away from her, because she was a bad mom for being
 11 a drug-seeking behavior person.
 12 So it took her three months and a DNA test and
 13 working directly with the state attorney general to get
 14 cleared and to get her kids back. So medical identity
 15 theft poses extraordinary harms to its victims, and
 16 Acting Chairman Ohlhausen discussed quantifiable risks.
 17 We released a report today called The Geography
 18 of Medical Identity Theft where we worked very hard to
 19 quantify the patterns and distribution of medical forms
 20 of identity theft. When medical identity theft happens,
 21 it usually happens by the actions of organized crime or
 22 various organized professionals who are working within
 23 medical and billing systems to create false billing
 24 situations. Sometimes it's the action of rogue
 25 individuals, like the woman who had a problem in Utah,

19

1 but no matter how it happens, people who have had their
 2 identity used by others to procure or bill for medical
 3 goods and services that they themselves did not seek,
 4 nor receive, have unique harms.
 5 The first core harm that they have is that
 6 fictitious entries are entered into their medical file.
 7 Typically, it's a very expensive disease, for example,
 8 HIV/AIDS, sometimes cancer treatments. A popular thing
 9 to add to victims' files is hepatitis C treatment
 10 because it can run up to about a thousand dollars a
 11 pill, leading up to about \$120,000 that people
 12 committing the crime can pocket for themselves.
 13 Meanwhile, the victim is left with hepatitis C on their
 14 medical file, not a great thing to have there for all
 15 sorts of reasons.
 16 So what on earth do these victims do to get
 17 cured? Well, unfortunately, there's no legal recourse
 18 to correct or delete medical information from files.
 19 Our geographic research that we published today shows
 20 that medical identity theft is, in fact, growing, but
 21 it's also doing something unique. It's growing in very
 22 specific regions of the U.S., for example, Florida and
 23 other areas where there are elderly residents that are
 24 clustered. And what is happening is that this crime is
 25 victimizing certain states, certain genders, certain

20

1 ages, the very young, the very old, and what's happening
 2 is that you're seeing real pockets of quantifiable harm.
 3 So let me move to the slides very, very quickly,
 4 and let's see if this works. Oh, it's going to work,
 5 okay. (Slide 6) So we did a very substantive
 6 statistical analysis, culling through almost -- well,
 7 just loads and loads of complaints to the Consumer
 8 Financial Protection Bureau.
 9 Now, these particular complaints are just the
 10 simple count of reports. So, in other words, these are
 11 the pure counts. If you look at this diagram, you can
 12 see California, because they are a populous state, they
 13 have got a huge roster of counts. The same with Texas
 14 and the same with Florida. You can see Georgia popping
 15 up there a little bit and New York. This is -- this is
 16 showing activity based on population.
 17 But when you normalize the data and adjust it to
 18 count per 1 million, all of a sudden the population
 19 density issue goes away, and what you get is this. So
 20 now you have a different picture emerging. (Slide 7)
 21 What you see here -- and by the way, the report has 2017
 22 data -- what you see here is an absolute crisis. You
 23 see a very deep distribution of medical identity theft
 24 across the U.S.
 25 You can see, for example, Nevada, Colorado,

1 Florida remains very high, and actually when you're able
 2 to look at the data closely, the entire Southeastern
 3 chunk of the United States is a hot spot for medical
 4 identity theft crimes and, in particular, Florida.
 5 (Slide 8) So here is a simple count of reports
 6 from 2016. This is, again, just a pure count, and I
 7 chose this to show you just so you could get a feel for,
 8 like, when people talk about medical identity theft, oh,
 9 California has a lot of cases. You see a lot of DOJ
 10 activity in California because there are so many cases,
 11 but then if you normalize the data, that's what you get,
 12 and you get these profound patterns where serious harm
 13 is happening.
 14 (Slide 9) People are having their health records
 15 falsified. People who -- in our research for this
 16 report, we found that people are literally unable to
 17 remove false billing records from debt collector
 18 scenarios. So these are profound harms. They are being
 19 targeted geographically, and consumers and patients who
 20 live in these hot zones are going to experience greater
 21 risk than those, for example, who live in North Dakota.
 22 And it's not just based on population; it's based on
 23 targeting.
 24 So I want to quickly pivot to biometric identity
 25 theft. We are behind the eight ball in the realm of

1 medical identity theft. It's in crisis proportions. In
 2 biometric forms of identity theft, we will certainly
 3 wish that we will have -- would have dealt with it
 4 early. We still can, and so that's why I'm very keen to
 5 present this to you.
 6 In biometric expert circles, there is something
 7 that's being talked about a lot, and we are
 8 unfortunately already seeing forms of this crime
 9 occurring. So what's happening is that healthcare
 10 providers are installing -- and others, schools and
 11 financial institutions and even federal agencies and
 12 other areas -- are installing biometric measures to
 13 ensure identity.
 14 So it could be an iris scan, it can be a
 15 fingerprint, can be facial recognition, all sorts of
 16 things, but the way that biometrics work, it's math,
 17 it's not magic, and it can be spoofed, and it can be
 18 foiled. This is one of the most difficult types of
 19 identity theft to prove your innocence of.
 20 (Slide 10) So what you're seeing right now, so
 21 on -- if you see subject one, subject one is -- let's
 22 just say that his identity information is stored in a
 23 hospital. Well, subject two comes along, and he's like,
 24 oh, you know what, I would really like some free
 25 healthcare, or I would at least like to do some fake

1 billing so I can sell some, you know, things on the
 2 street. So let me -- you know, this hospital has an
 3 enrollment -- a biometric enrollment system. Let me go
 4 ahead and, you know, take his, you know, driver's
 5 license scan that the hospital so helpfully has stored
 6 for me, and let me use free technology to morph my photo
 7 with his, and we will create that middle image that you
 8 see, morph one plus two.
 9 Well, unfortunately, it is very unambiguous
 10 research at this point that subject one, with the
 11 original photo, and subject two, with the -- his
 12 original photo, based on that center morphed photo, both
 13 of those subjects will be authenticated within that
 14 healthcare system. So what we are seeing on the street
 15 now is clinics and other kind of bad actors taking
 16 biometrically morphed authentications and stringing a
 17 dozen people off of that authentication and passing
 18 people through. So this is a risk that has not made it
 19 into the mainstream yet, but we are watching it very
 20 closely.
 21 So based on these things, I have just a couple of
 22 things I want to say in terms of harms and what to do.
 23 It is very clear that victims of medical identity theft
 24 and advanced forms of identity theft like that have
 25 experienced very different harms than victims of lesser

1 forms of identity theft, such as credit card fraud.
 2 They are in a class by themselves, and I call on the FTC
 3 to study and treat this form of identity theft as a
 4 completely distinct and separate class, because there
 5 are completely distinct and separate classes of harms,
 6 and Congress definitely needs to pass specific
 7 legislation in terms of working to create remedies for
 8 these situations.
 9 It will require dedicated work from the FTC and
 10 other federal agencies, including CMS, working directly
 11 with state-level AGs, because of the patterning of
 12 medical identity theft. For biometric harms, it's going
 13 to take a lot of money, because these presentation
 14 attacks through biometric morphing, the only way you can
 15 fix it really is to have a secure line where you have a
 16 secure photo, not a Kinko's photo or a photo taken at an
 17 insta-passport place or somewhere else, but you have a
 18 secure photo that goes securely to whatever vendor is
 19 creating the -- you know, the final product.
 20 These systems are easy to spoof also in other
 21 ways. So if someone has taken over your biometric
 22 identity, it's very hard to prove your innocence. These
 23 are distinct harms. We've got to study them, benchmark
 24 them, and work very diligently on their specific and
 25 unique harms. We can't lump identity theft as a

1 category together anymore.
 2 MS. CONNOR: Thank you, Pam. If you can pass the
 3 clicker on to Damon.
 4 So Damon, as we just heard about medical and
 5 biometric identity theft, those might be new topics to
 6 some, but it's fair to say that most people know at
 7 least a little bit about identity theft; however, there
 8 are still abuses of personal information out there that
 9 people may not know about but that are incredibly
 10 damaging to people. Can you explain what some of those
 11 are?
 12 MR. MCCOY: Sure. I am going to go through a
 13 little bit of the research that I've been doing on this,
 14 kind of starting with what's called doxing, and so
 15 doxing is basically the public release of people's
 16 information that they probably wish to keep private.
 17 (Slide 11) And so for those of you that haven't stared
 18 at lots of these doxings, these doxings are posted a
 19 surprising amount of times on the internet, and these
 20 doxes normally include the names of the people, their
 21 online aliases, their age, their date of birth, their
 22 addresses, phone numbers, sometimes medical kinds of
 23 information about them, ISP information, and also a lot
 24 of information on the family of these victims. And it
 25 also includes things like their online social networking

1 profiles and things like this.
 2 (Slide 12) And so these doxings are oftentimes
 3 posted with the hope that they're trying to encourage
 4 harassment of the victims of these doxings. And so in
 5 one of my studies, we actually built a system based on
 6 some machine learning that was able to go out and find
 7 about 6000 of these doxings. So we ran the system for
 8 about 12 weeks, and we found 6000 of these doxings, and
 9 probably the ones that we found were only the most
 10 egregious of these doxings since our system was fairly
 11 conservative about what it calls a dox. And so based on
 12 this, we could do some analysis of these doxes.
 13 What we find is that the victims often come from
 14 one of two communities. They either come from the
 15 gaming community, video gamers, or they come from the
 16 community of kinds of hackers and underground kinds of
 17 actors. The other thing we can see from this is that
 18 the victims oftentimes skew very young, and so the
 19 victims are oftentimes in their teens, perhaps in their
 20 early twenties, something like this as well. So this is
 21 very targeted and impacting, not the people likely in
 22 this room, but kind of the younger generation of people.
 23 As you can see from the, you know, 6000 doxes that we
 24 found -- and this was not a comprehensive study -- that
 25 this is happening very frequently and impacting a lot of

1 people's lives.
 2 (Slide 13) And so one of the probably most
 3 egregious harms that can happen from this is in those
 4 doxes, again, they include people's social networking
 5 profiles, and, again, this is done to kind of encourage
 6 other people to pile on and harass these people. So
 7 what you're looking at here is -- we actually did our
 8 study in two parts. So we did our study in two six-week
 9 parts. We found about the same number of doxes in each
 10 part of our study, and with these social networking
 11 handles, we pulled these out of the doxes automatically
 12 and we monitored the privacy settings of these people's
 13 accounts.
 14 What you can see from this graph here on that
 15 first one is that red part is essentially people closing
 16 their accounts down, so this represents people becoming
 17 socially isolated, likely being forced by harassment to
 18 close their Facebook accounts because of these doxes.
 19 And so what you can see in that first period is that --
 20 and the thickness of this is the magnitude of the number
 21 of accounts that are closing it down. And so that first
 22 part is before Facebook started deploying filtering to
 23 try and filter out harassing comments from their
 24 platform, and that second part is after Facebook
 25 deployed filters to filter out harassing comments from

1 these. And you can see the huge benefit that was
 2 incurred by their population when Facebook did this.
 3 This was actually kind of a nice thing. Then we can
 4 show that this kind of harm can perhaps be mitigated by
 5 these filters that these online social networking sites
 6 are deploying.
 7 (Slide 14) The other kinds of harm, probably the
 8 much more dangerous kinds of harms that can come from
 9 these is, again, the phone numbers, addresses, are also
 10 included in these doxes, and so this can lead from
 11 fairly innocuous things from someone ordering a pizza to
 12 someone's house to someone creating kind of a fake
 13 emergency situation, say, like, they make up a situation
 14 where it's a hostage situation or something like that,
 15 and they call up, you know, 911, and they say there's a
 16 hostage situation going on in this house.
 17 This triggers a response by the Police Department
 18 to send, you know, armored swat teams to someone's house
 19 with guns blazing, on to someone's house, and this has
 20 resulted in many dangerous kinds of situations.
 21 Unfortunately, this kind of harm is more difficult to
 22 try and measure, but I think this is something that we
 23 should do a better job, from police databases and things
 24 like that, to measure this type of harm that's incurred
 25 by doxes.

1 And so the other question is, right, where are
 2 they getting this information from? And so one thing
 3 that we can notice from these doxes is that a lot of
 4 times they have ISP information, and a lot of times
 5 there's also online cookbooks as to how to gain
 6 information to dox people. A lot of times these include
 7 a method where they essentially socially engineer call
 8 support centers, especially ISP call support centers.
 9 So they can start with someone's IP address that
 10 they somehow gained maybe by playing a video game with
 11 them, and they can spider out and start to get more
 12 information. So this is another thing where we should
 13 investigate how they are getting this information and
 14 perhaps understand how to make it more difficult for
 15 them to acquire information this easily.
 16 (Slide 15) The other way that they acquire
 17 information is by sometimes socially engineering their
 18 victims into installing malware, and it's a particular
 19 kind of malware that they normally have installed on the
 20 victim's machine that's called a remote access trojan,
 21 or RAT for short.
 22 So there's unfortunately underground ecosystems
 23 where the doxes are posted. So there's other hacker
 24 forums where they basically trade or talk about how to
 25 acquire victims, which they called slaves, to infect

1 with these remote access trojans. And when a victim is
 2 infected with one of these remote access trojans, this
 3 effectively gives the hacker complete access to that
 4 person's computer, including the camera, the microphone,
 5 all of the files on the system, the attacker can rummage
 6 through.
 7 (Slide 16) So oftentimes what crops up from this
 8 is what we called sextortion, where the attacker somehow
 9 steals some sensitive information from the victims and
 10 tries to extort them for more images or perhaps for
 11 money and things like this. So a high-profile victim of
 12 this was Miss Teen USA. She was infected by one of
 13 these RATs, and she was caught up in one of these
 14 sextortion cases, but there are hundreds and hundreds of
 15 these victims.
 16 So, in fact, we did a study where we enticed
 17 attackers to attack our own system, and we had over
 18 hundreds of attackers, unique attackers, that visited
 19 our systems, many of them from the U.S., but from all
 20 over the world, and the first thing that most of the
 21 attackers did is they tried to access our camera when
 22 they attacked our systems.
 23 (Slide 17) And so the final thing that we have
 24 been looking at lately is spyware. I think actually
 25 spyware is kind of a misnomer for this. I oftentimes

1 called it stalkerware or something like this. So these
 2 are mobile apps that can be installed on people's
 3 phones. Some of these are in, say, the Play Store and
 4 Apple's App Store, and they have kind of dual-use
 5 features.
 6 So they can be used, for instance, to find
 7 someone's stolen phone or they can be used to kind of --
 8 without the victim's consent, to stalk them, and things
 9 like that. And then there's stuff that's off of these
 10 stores that's much more egregious. And so a lot of
 11 these developers, as you can see from this marketing
 12 material that I have posted up here, are essentially
 13 encouraging people to use it for this use case of
 14 stalking their partners, and so this can lead to a lot
 15 of different kinds of harms. Probably the worst of
 16 these harms is interpartner violence, so this can be
 17 used to facilitate intimate partner violence. It can
 18 also be used, again, to stalk people and things like
 19 that.
 20 And so doing just quick internet searches, you
 21 can find, you know, tens to hundreds of these different
 22 apps that abusers are talking about installing on their
 23 victims' phones and things like that. And, again, we
 24 can see paid advertising where the developers of these
 25 kinds of stalkerware apps are encouraging and

1 facilitating this use of their apps.
 2 And so throughout all of these studies, I can
 3 kind of show that oftentimes there are cyber harms that
 4 are hard to kind of boil down to dollars. They are, you
 5 know, physical threats and things like this, emotional
 6 harm, social isolation, that are very hard to kind of
 7 boil down into dollars, and they affect oftentimes young
 8 people and things like that, so the newer generation,
 9 and they probably have a lifetime of impact against
 10 these people that are harmed by these kinds of cyber
 11 attacks.
 12 And so with that I would kind of encourage more
 13 of these kinds of studies to kind of understand the
 14 scale and other kinds of harms that are occurring with
 15 this and also the intermediaries that are kind of
 16 facilitating these kinds of harms. So with that I will
 17 hand it off.
 18 MS. CONNOR: Thank you, Damon.
 19 So, Lauren, so far we have discussed injuries
 20 that occur to particular consumers, but what kind of
 21 informational injuries are possible when many consumers'
 22 information is combined?
 23 MS. SMITH: Great. Well, thank you for having me
 24 here to speak today. I'm excited to participate in the
 25 panel. So, yes, I am going to take a little bit of a

1 broader view, to take a step back, and think about the
 2 fact that as the volume of consumer data grows, the
 3 number of decisions that were previously made by humans
 4 are now increasingly being made by algorithms. As the
 5 number of data sources have multiplied, so, too, have
 6 the types of data involved in these decisions and the
 7 number of entities that may process and analyze this
 8 data across many sectors.

9 So I am going to be talking about potential harms
 10 that come not just from explicitly fraudulent activities
 11 or hostile approaches that we have heard from some of
 12 the other panelists today, but instead look at, you
 13 know, areas where the collection of the data initially
 14 may have been legitimate uses, may have been offered up
 15 by consumers in exchange for a service.

16 As you mentioned, this can create a number of
 17 sort of downstream effects. So information can be
 18 combined, so a consumer may provide some information in
 19 some context, but in what is sometimes called the mosaic
 20 effect, the information could be combined with other
 21 data sets and perhaps reveal information that they may
 22 not wish to have out there publicly, and also there can
 23 be inferences based on data that consumers have shared,
 24 you know, particularly with the advance of artificial
 25 intelligence, that there may be information that could

1 be inferred about a person from data about themselves
 2 that they may not have explicitly shared.

3 So in a lot of instances, analysis of sensitive
 4 data categories, such as race, gender, pregnancy status,
 5 can be used to improve services, promote inclusion,
 6 advance research, and actually be used to mitigate human
 7 bias, but in other contexts, it can raise the specter of
 8 disparate impacts on vulnerable communities.

9 As a number of folks have sat down to try to
 10 tackle this issue, I know my initial work on this
 11 started when the White House did a report on big data,
 12 looking at the benefits and potential risks arising from
 13 big data, and one of the biggest areas that was sort of
 14 a surprise to the folks working on this project and in
 15 the building was the intersection of big data and civil
 16 rights and the way in which this growth in automated
 17 decision-making could wind up impacting civil rights.
 18 The FTC has also done a lot of good work and hosted a
 19 workshop on that topic explicitly.

20 So as my organization sat down to try to tackle
 21 this issue, we found that conversations on the topic
 22 sometimes become mired in definitional challenges that
 23 can make progress toward solutions difficult. So these
 24 analyses sometimes fail to separate harms from the
 25 causes and from solutions. Sometimes we wind up

1 conflating human biases that have shaped society for
 2 years with digital causes. This can make it difficult
 3 for a consumer protection agency, like the FTC, to
 4 determine what kind of injury they should be protecting
 5 consumers from and how to define that.

6 So, you know, identifying financial injury around
 7 fraud, breach, or security failures may be fairly well
 8 defined, as we've seen in several FTC enforcement
 9 actions, but in other contexts, identifying the injury
 10 may be more complex. We can run into issues like this
 11 with things like differential pricing, which has given
 12 us things like senior and student discounts for years
 13 without, you know, creating what we might consider to be
 14 a financial injury, but can raise new concerns as
 15 consumer purchasing moves to the internet and pricing
 16 can shift based on a range of consumer attributes.

17 So we've found that there aren't many easy ways
 18 to navigate these issues, but we think that more can be
 19 done to promote fairness and encourage responsible data
 20 use. So to facilitate these conversations, we
 21 endeavored on a project that launched today, that I'll
 22 give you a brief preview of, and there are handouts also
 23 at the front. (Slide 18) We reviewed the leading books
 24 and articles on this topic and tried to distill the
 25 different harms that are identified in the literature

1 into a set of buckets and into a chart so that we could
 2 think about them at a very high level and try to
 3 understand what are the types of harms that could arise
 4 from automated decision-making based on consumer data,
 5 so that we could have them all in one place and
 6 determine whether some of them should be considered more
 7 of a risk, more important to address and focus on than
 8 others, and whether mitigation strategies might differ
 9 depending on which types of harms you're talking about.

10 So you can see a bit on this chart up on the
 11 screen, and so the first distinction that we made in
 12 groups of harms was the types of algorithmic
 13 decision-making that could either turbocharge or make
 14 more opaque harms to individuals, which you will see is
 15 the left two-thirds of the chart. And on the right is
 16 collective harms, which may be a little more difficult
 17 to pinpoint because there may not be, you know, specific
 18 harm to a particular person but may impact us at the
 19 group level, either as a society as a collective or
 20 specific groups.

21 And for the first, under individual harms, we
 22 drew a distinction between those that are unfair and
 23 those that are illegal, because we felt that there is
 24 sort of more clarity in especially civil rights law, as
 25 well as, you know, FCRA and some other areas where

1 specific harms to an individual could be -- have already
 2 been identified as illegal, as there is sort of a clear
 3 societal consensus that we do not want these harms to
 4 occur and can use technology to ferret out and to
 5 prevent some of those harms.
 6 And then the ones that are not as explicitly
 7 illegal can raise questions of unfairness and of ethics
 8 but may require us to do a little more thinking to
 9 determine, you know, in what instances this would be
 10 considered an injury to consumers and how one might want
 11 to think about identifying and mitigating and being
 12 aware of some of those concerns that might arise with
 13 automated decision-making overall.
 14 So when we got to the substantive grouping of the
 15 harms, we found that, by and large, they could be
 16 grouped into four broad buckets. So the buckets are
 17 loss of opportunity, economic loss, social detriment,
 18 and loss of liberty. We thought that these depicted the
 19 spheres of life where automated decision-making could
 20 potentially cause the most harm.
 21 In any of these buckets, as I mentioned, the harm
 22 could be illegal, it could be not illegal; it could
 23 accrue wholly to the individual or to a group. So, you
 24 know, an example of an individual harm could be me not
 25 being able to rent an apartment because of a decision

1 made about me or something entirely to society, which
 2 could be something like filter bubbles that have become
 3 a topic of discussion, especially around the election,
 4 that many of us may believe have a harmful impact on
 5 society overall but have not been distilled as clearly,
 6 at least in existing law, and may not be something that
 7 can be tackled at that level at this point.
 8 So for loss of opportunity harms, this group
 9 broadly describes harms that occur within domains of
 10 workplace, housing, social support systems, healthcare
 11 and education. Economic loss harms broadly includes
 12 harms that cause financial injury or discrimination in
 13 the marketplace for goods and services. Social
 14 detriment largely talks about harms to one's sense of
 15 self, self worth, or community standing relative to
 16 others. And loss of liberty applies to harms that
 17 constrain one's physical freedom and autonomy.
 18 So these are up on the screen. In our packet, we
 19 give particular examples of each of these, and I'm happy
 20 to run through those individually. You know, we
 21 recognize that these categories that I just ran through
 22 aren't mutually exclusive, you know, economic loss can
 23 certainly lead to loss of opportunity, but in our
 24 attempts to sort of survey the literature and boil these
 25 down, we found these to be the most ready categories.

1 And then in an accompanying project, we also used
 2 these categories to then try to bucket the harms into
 3 different groups that can be approached with the same
 4 sets of mitigation strategies depending on the way
 5 they're characterized in this chart.
 6 MS. CONNOR: Thank you, Lauren.
 7 Cindy, given your experience with domestic
 8 violence victims, what types of informational injuries
 9 do you see arising and how?
 10 MS. SOUTHWORTH: I just wanted to take a moment
 11 to go back to the "Hello Spy" slide that Damon provided,
 12 because it gives me great pleasure to trash them at
 13 every chance I get, because we proudly tweet at them.
 14 They are foul human beings. This is how they advertise
 15 an alleged family safety product. It's all about
 16 encouraging and facilitating stalking and domestic
 17 violence. So I last trashed them in 2014 at a Senate
 18 hearing, but I appreciate any opportunity to go after
 19 miscreants like this.
 20 On a more serious note, just a little bit about
 21 domestic violence, stalking, and sexual violence. Many
 22 people think of them as these, like, tiny societal
 23 issues, this fringe thing, and when you actually look at
 24 CDC, FBI numbers, Department of Justice research, one in
 25 four women will be physically assaulted -- physically

1 assaulted -- by an intimate partner at some point in her
 2 lifetime. That doesn't count emotional abuse and
 3 control and lots of other unhealthy and controlling
 4 relationships. One in six women will be stalked by a
 5 partner or stalked, and one in 19 men will be stalked in
 6 their lifetime. And then one in three girls will be
 7 sexually abused before they're 18 and one in six boys.
 8 Those are staggering numbers. That means your
 9 CEO, your boss, your neighbor, your friend, your postal
 10 worker, your, you know, barista at the Starbucks, your
 11 next politician is a survivor of one of these crimes.
 12 And so when you think about this large swath of society
 13 who's experienced significant victimization, then you
 14 think about how they're part of our daily lives, they're
 15 part of our data sets, they're part of our medical
 16 records, they're part of our lives.
 17 And so the Safety Net Technology project that I
 18 founded 17 years ago on our blog, techsafety.org, we did
 19 a survey back in 2014, and we found that the local
 20 domestic violence organizations -- there's about 2000 of
 21 them nationwide that take those hotline calls from
 22 victims who are experiencing pretty horrific things --
 23 and back in 2014, 97 percent of those front line victim
 24 service organizations said they were seeing cases where
 25 tech was being misused by offenders and abusers. Of

1 course, because tech is part of all of our lives. We
 2 all have our hands right next to a phone.
 3 And three years ago, in that same survey, we
 4 found that 71 percent, almost three-quarters of those
 5 local programs, said that abusers and stalkers had
 6 started using technology to monitor internet and
 7 computer use, so essentially spyware. We don't have
 8 prevalence or incidence stats. This is just what the
 9 victim advocates are seeing on the ground, and the
 10 numbers are really quite concerning.
 11 When you think about some of the specific harms,
 12 the obvious one is, you know, illustrated above. It's
 13 the physical harm. People running for their lives still
 14 happens, you know, domestic violence shelters end up
 15 housing or supporting 72,000 adults and victims in a
 16 given 24-hour period, but 41,000 adults and kids are
 17 kept safe in a shelter or a transitional housing program
 18 on a given day, 41,000 people. So they have significant
 19 privacy needs, and they are obviously quite concerned
 20 about data privacy and data security.
 21 Some of the other things that can happen that you
 22 need to think about are credit issues. We find one of
 23 the most common tactics by abusers is to ruin a victim's
 24 credit, and so then if you have got commingled credit,
 25 if the abuser's criminal records get commingled with her

1 records in some way, or his records if he's the victim,
 2 those are really challenging things that can have
 3 devastating consequences.
 4 You have job loss that you can have if you are
 5 identified as a victim. Unfortunately, there's still a
 6 huge stigma. Some people will say it's not safe for you
 7 to work here, you might be a risk to your colleagues, so
 8 you see all sorts of discrimination type things that
 9 Heather is going to be touching on more.
 10 Other things to think about is just how data in
 11 combination can be problematic. And so years ago AOL
 12 released some of their search data for research purposes
 13 and didn't realize how identifying it was. A reporter
 14 actually took that data set, realized that somebody was
 15 searching for themselves by name and also searching for
 16 things like domestic violence, shelter, protection
 17 orders.
 18 So the reporter called the victim up and said,
 19 hey, I got your information from the AOL search data
 20 set. Are you a victim of domestic violence? And, of
 21 course, she was. So how sort of crazy that would be to
 22 have a reporter call up and say, hey, I figured you out.
 23 Are you a victim? And given the stigma that is still
 24 out there, that is incredibly concerning.
 25 Some of the other things to think about is not

1 just physical harm, but some of the data that victims
 2 are most concerned about is their home address. And so
 3 when medical records started becoming a real issue, one
 4 of the things people were sort of caught up on is the
 5 sensitivity of what's in a medical record, diagnoses,
 6 medical treatment, and, of course, that's true.
 7 But for a victim of domestic violence or stalking
 8 who's literally on the run or living in hiding or trying
 9 to rebuild a life, just the home address being
 10 compromised, shared, you know, in any way, either
 11 through legitimate or illegitimate means, that could put
 12 a victim's life in danger, and then they may have to
 13 move.
 14 And so when you talk about cost, it's, you know,
 15 physical cost of relocation, of plane tickets, bus
 16 tickets, movers, alarm systems, changing door locks,
 17 slashed tires. So those are the types of things that we
 18 see when there's privacy and security breaches.
 19 MS. CONNOR: Thank you, Cindy.
 20 And last but not least, Heather. Given your
 21 experiences, what kind of injuries result from the
 22 disclosure of medical information, sexual orientation,
 23 or gender identity that a consumer prefers to keep
 24 private?
 25 And then to go beyond that, what are the effects

1 when people fear that this information, this medical
 2 information, sexual orientation, or gender identity, may
 3 be disclosed?
 4 MS. WYDRA: Yeah. Thanks very much for having me
 5 here. I am happy to talk about these issues. I am an
 6 attorney at Whitman-Walker Health. We are a medical-
 7 legal partnership where we provide medical services to
 8 anyone living with HIV in the greater D.C. community and
 9 anybody identifying as LGBTQ, again, in the greater D.C.
 10 community.
 11 So the reason that brings me here to this panel
 12 is because a large part of what I do in the legal
 13 services program is to counsel and represent people who
 14 have been affected by a disclosure of personal
 15 information, a disclosure of, for example, personal
 16 health information, private health information, or a
 17 disclosure of gender identity and sexual orientation
 18 that the person did not want to be disclosed.
 19 And I see people harmed by these disclosures --
 20 well, in countless contexts, but the three I'll talk
 21 about today are in the workplace, places of public
 22 accommodation, and then in an interference with personal
 23 relationships, and that can be in the home, in the
 24 community, in the workplace, and elsewhere.
 25 So to begin to talk about the workplace, a large

1 part of what I do is employment discrimination, and a
 2 lot of times discrimination starts when somebody's
 3 health information -- in a lot of cases with the clients
 4 that I work with it's HIV, it could be something else --
 5 is disclosed in the workplace. And sometimes the
 6 disclosure is necessary, sometimes it isn't, but
 7 regardless, the results are not always positive.
 8 And the negative effects can be seen in every
 9 aspect, at every stage of the employment relationship.
 10 I have had clients who have come to me who have gotten
 11 through the initial portions of a job application, and
 12 then as you get a little bit further in the process,
 13 when you have what's called a conditional offer of
 14 employment, the employer is then allowed to ask for
 15 health information, can ask about HIV status, and can
 16 even make people undergo an HIV test as long as everyone
 17 who is applying for that position is required to do the
 18 same thing. An employer can't pick and choose.
 19 And then, believe it or not, it still happens,
 20 after that testing occurs, after somebody's status is
 21 public, they find themselves suddenly without a job
 22 offer. That's illegal. Of course, it's illegal, but
 23 sometimes it still happens. Then it becomes my job to
 24 prove that the withdrawal of the offer was based on the
 25 HIV and not for some other purpose. That's a blatant

1 example.
 2 Another one that can be more subtle but still
 3 happens is I worked with a client who was applying to be
 4 a bus driver in one of our nearby counties and, again,
 5 had to fill out a huge medical questionnaire. It didn't
 6 actually ask about HIV, although it could have, that
 7 would have been permissible, but she ended up disclosing
 8 it just because she had some blood work that was coming
 9 back oddly and thought, well, maybe if I just say this,
 10 this will end all of the inquisition.
 11 But the doctor, instead of saying, okay, now I
 12 understand, she had letters from her personal physicians
 13 clearing her to do this job, said, well, I want you to
 14 go back and get these three tests, and I need all of
 15 these records. And eventually my client said, you know,
 16 they don't want me here, and I don't want this job.
 17 They don't want me here. So that's another example.
 18 And then the example that I really see the most
 19 is someone who's going about their day, doing their job.
 20 I worked recently with somebody who's a maintenance
 21 worker in an apartment complex, and because he had to
 22 take so much time off for doctors' appointments, he
 23 finally said to his supervisor, you know, I'm positive.
 24 I've got to go to the doctor. I've got to get blood
 25 work. I have to have these medication checks.

1 Well, he didn't get fired, but all of a sudden,
 2 nobody wanted to work with him anymore, and he was put
 3 on these assignments by himself, and people said strange
 4 things to him, like, shouldn't you be wearing gloves?
 5 And day after day, there was just some little indignity
 6 that he had to endure. So, you know, in that kind of
 7 thing, I mean, yeah, there's a hostile work environment
 8 claim that we can bring, but, you know, it can be hard
 9 to find a remedy for that, and it's just something that
 10 he had to endure.
 11 So the next context that I'll talk about where I
 12 see harm occurring is in what we call places of public
 13 accommodation. So that is any place that people go, you
 14 know, restaurants, hotels, gyms. The example I am going
 15 to talk about is the gym, and I am going to use the
 16 example of somebody who was transgender.
 17 I worked recently with a client who was going to
 18 her gym, having absolutely no problem. She was a
 19 transgender female. So just to give you your Trans 101
 20 training, that means she was born -- she was identified
 21 as male at birth but had been living outwardly as female
 22 for years, but she hadn't changed her driver's license.
 23 So she was going to the gym, using the women's locker
 24 room, everything was fine, but then one day she didn't
 25 have her ID card and had to show her driver's license,

1 which was old, had an old picture, had an old name, and
 2 after that, everything changed. The manager said she
 3 couldn't use the women's locker room anymore. So we're
 4 currently dealing with that case.
 5 As some of you may know, in D.C., the law is very
 6 clear. It doesn't matter whether identity documents are
 7 formally changed or not. If somebody identifies as male
 8 or female, that is the gender where they need to be
 9 treated under the law.
 10 And so, finally, I'll talk about the harm that
 11 can come in personal relationships when personal
 12 information is disclosed. There was an incident that
 13 happened with Aetna. It was in the news. It was
 14 public. Aetna sent a mailing to dozens of its
 15 HIV-positive clientele who were -- they were making some
 16 change to how they were covering HIV medications, and
 17 the mailing that went out had a very large window that
 18 shows the address, you know, where you can see what the
 19 address is. The window was so big that it actually
 20 showed the first couple sentences of the letter, which
 21 talked about HIV and medication.
 22 Well, these letters went to people at their
 23 homes. They went to people at their apartment
 24 complexes, where, you know, mail is just thrown
 25 everywhere by the front door. A lot of people ended up

1 with their personal health information disclosed to
 2 family members, neighbors, friends, when they really
 3 didn't want it to.
 4 Sometimes that was okay, but we heard horrible
 5 stories, people who came to us wondering what they could
 6 do, because -- I mean, again, it ran the gamut from, you
 7 know, people just look at me weird now to somebody
 8 wrote, you know, bad words across my apartment door and
 9 vandalized my garden and left me notes saying we don't
 10 want your kind here.
 11 So those are the types of things that can happen
 12 to people when their personal information is disclosed
 13 without their permission.
 14 MR. WOOD: Okay. Well, thank you very much,
 15 Heather, and thank you to all the panelists for
 16 describing to us a very wide range of injuries. I
 17 hesitate to ask, but are there other types of
 18 informational injuries that we haven't touched on yet?
 19 MS. DIXON: Well, if no one is going to respond,
 20 I will. There are certainly more types of informational
 21 injuries, and they are hiding in every corner of the
 22 digital ecosystem. I think, though, that the important
 23 thing is to focus on what causes substantive harm and
 24 harm that has meaningful impacts on a person's life.
 25 You know, we can all spend time working on

1 issues, but there are big issues. I do think that
 2 medical forms of identity theft, I think biometric
 3 harms, I think these are big issues. I think the issues
 4 we've heard around this table are big issues. If
 5 someone is going to have their life threatened or their
 6 livelihood threatened, these are profound harms.
 7 So in some ways, I mean, it's -- I would really
 8 rather look at quality and say, look, here are very
 9 meaningful harms that we have quantified, we've studied,
 10 we know about, so let's roll up our sleeves and let's do
 11 something about them. We've had plenty of time to
 12 identify these harms. Why not have the FTC write a new
 13 report, for example, about domestic violence, about
 14 medical identity theft, about these other harms? Hold a
 15 separate workshop. Let's find solutions. Let's work
 16 collaboratively. I'm all for it. Instead of, you know,
 17 breadth, let's go depth, and let's solve the problems.
 18 MS. SMITH: I would say one area of harms that we
 19 haven't provided examples on yet up here are the loss of
 20 liberty harms that can have a very significant impact on
 21 folks' lives. So there has been a lot of good research
 22 on predictive policing and the fact that relying on data
 23 to determine how policing resources are targeted can
 24 reproduce -- if it's not done with an understanding of
 25 the risks, can reproduce historical bias and have very

1 significant impacts on communities at large.
 2 I think those are, you know, things we're just
 3 beginning to understand and figuring out how to
 4 mitigate, and things like use of recidivism scores,
 5 making sure we're understanding the type of data that is
 6 going in, assessing whether that is the correct data,
 7 assessing whether that data has its own biases built
 8 into it when we're making decisions about folks' literal
 9 freedoms.
 10 MS. SOUTHWORTH: Just on that note around sort of
 11 what police data can do, police data can do a lot of
 12 mitigation of harms in terms of helping identify where
 13 you have got either overpolicing or underpolicing or
 14 institutional bias dilemmas. One of the downsides of
 15 police data is, inadvertently, it can actually be
 16 identifying.
 17 So there was a 12-year-old rape victim that
 18 was -- her identity was basically compromised by a very
 19 well-intentioned police department publishing their
 20 police data, and they used the block to try to anonymize
 21 the data, but there was only one adolescent girl on that
 22 block. So even, you know, the attempts to an anonymize
 23 the data just -- it wasn't anonymized, and so in that
 24 case a pretty traumatic life experience then became
 25 amplified by the whole world finding out about it.

1 MS. CONNOR: So we have been talking a bit about
 2 the actual injuries that come after the fact, but what
 3 about -- and we have heard a little bit about the risks
 4 of injuries, but I guess for Heather and Cindy, I'm
 5 wondering if the people that you work with, if you see
 6 them acting differently or, you know, are they not --
 7 are they afraid to give and use their information for
 8 positive purposes to help them because they are afraid
 9 it's going to be misused in some way?
 10 MS. WYDRA: Yeah, I can start with that, and,
 11 Cindy, I'm sure you will have plenty to add.
 12 Absolutely. Where I see that a lot is in the area of
 13 healthcare, especially with people who have experienced
 14 discrimination someplace else, will be afraid to go and
 15 see a doctor because they're worried that either a
 16 doctor won't want to treat them because they are
 17 HIV-positive -- and, yes, that still does happen -- or
 18 someone who is transgender feels, you know, like a
 19 doctor won't know what to do with me, they will be
 20 biased against me.
 21 There are plenty of instances of doctors being
 22 very culturally insensitive to someone who is
 23 transgender and not understanding at all what their
 24 particular medical needs are or even why someone would
 25 be transgender. So, yes, that is one area where I see

1 people then afraid to go for healthcare outside of
 2 Whitman-Walker.
 3 MS. SOUTHWORTH: There's a real conundrum. I
 4 know some of the attempts for data security have been to
 5 mail things to people's homes. That came up during some
 6 of the pretexting of phone records dilemmas, and from a
 7 domestic violence victim standpoint, that's not
 8 necessarily helpful.
 9 The same sort of scenario of somebody being
 10 afraid to go get healthcare after a victim is relocated
 11 to a different town because the health insurance will
 12 send notification of the care that was provided and the
 13 location of where it was provided to the original home
 14 address, and it's really hard as it is to safety plan
 15 with victims of domestic violence and stalking who are
 16 trying to relocate and sort of talk about make sure you
 17 grab the birth certificates, you know, get the favorite
 18 teddy bear, make sure you have got the bank records and
 19 all this, and oh, by the way, you need to notify the
 20 insurance company, this data broker, all these other
 21 places, and change your address.
 22 People are a little busy running for their lives
 23 to do all of those steps, so what on the one hand is an
 24 attempt to be providing transparent notification to the
 25 sort of address on record, it gets very challenging in

1 terms of other places where victims sort of opt out of
 2 society, sort of what Damon was showing in terms of
 3 after people are targeted, do they shut down their
 4 Facebook accounts, do they opt out of social media, do
 5 they choose to sort of exclude themselves, or are they
 6 told explicitly?
 7 We have had many survivors told by law
 8 enforcement, if you don't want to be threatened by your
 9 ex, get off Twitter or get off Facebook, which is
 10 isolating, especially if your entire family -- one of
 11 the ways that my now family communicates is I know who's
 12 expecting a baby because I'm on Facebook with all of my
 13 cousins and relatives.
 14 Telling me the only way I can be safe and be
 15 female in the world is to get off the internet because,
 16 well, this misogyny just happens, so just get over it
 17 and get offline, that's not possible and it's isolating.
 18 It also impacts job possibilities. If I can't safely
 19 use technology, I am far less likely to go get a
 20 well-paying job.
 21 MS. DIXON: I would like to add on to that very
 22 briefly. The other thing I see a lot in my work is that
 23 people don't understand what it is that will actually
 24 protect them meaningfully, as opposed to things that
 25 they just feel like will protect them. A really good

1 example of this are people who have had some kind of
 2 exposure that's problematic, and in order to reduce the
 3 information flows, I often recommend to them to actually
 4 opt out of certain websites. They won't do it because
 5 they don't want to give any additional information.
 6 So I've actually had people who refused to opt
 7 out of, for example, financial information sharing
 8 because they don't want to give their Social Security
 9 number. People are so afraid of giving their Social
 10 Security number, when in that instance it would actually
 11 help them.
 12 So I do think that there needs to be a lot better
 13 understanding of, okay, what piece of information can I
 14 give up that will actually help me? What pieces of
 15 information will genuinely be harmful? I'm not
 16 persuaded that, you know, getting off of all technology
 17 is the right answer here.
 18 I would really like to take the position that,
 19 look, let's be able to use technology and have it not
 20 harm us. That's really the situation I want to see
 21 people get to.
 22 MS. CONNOR: Thank you.
 23 So moving on a little bit, what are the costs of
 24 fixing these informational injuries that you've all been
 25 talking about, financial or otherwise? And I know

1 Heather was speaking to this a bit, about legal
 2 remedies, but what legal remedies are available to
 3 consumers to address these harms? And if there's not
 4 any, what gaps are there and what are their
 5 consequences? I know that's a loaded question, but...
 6 MS. WYDRA: Well, I can start talking about, you
 7 know, the clients that I work with and the cases that I
 8 see. The remedies, if they exist, they come under the
 9 state, local, and federal antidiscrimination laws. So
 10 that could be Title VII, that could be the Americans
 11 with Disabilities Act, and then the state counterparts,
 12 the D.C. Human Rights Act, the Maryland Civil Rights
 13 Act, and so forth. So that's one way for people to get
 14 a remedy.
 15 For the disclosure of medical information by a
 16 healthcare provider, there is HIPAA, but for those of
 17 you who know anything about HIPAA, it doesn't provide a
 18 remedy to the individual who has been harmed by the
 19 disclosure. It can provide a penalty and sanctions and
 20 other types of punishments to the medical provider or
 21 the insurance company, but the person who has been
 22 harmed, there is no remedy for them.
 23 And then, of course, you always -- there are some
 24 things that there is -- just no amount of money
 25 compensates for. I mean, you try, but loss of

1 reputation, emotional harm and suffering -- I mean,
 2 certainly, yes, we try and fix those things with
 3 financial remedies, but there are some things that can
 4 just never go back to the way they were before.
 5 MS. SMITH: So I think, you know, part of why we
 6 undertook this exercise is to understand that, depending
 7 on the type of harm, it may have a different set of
 8 remedies. So for some of the more well defined harms,
 9 such as employment discrimination, so even if there is
 10 existing law saying that a certain group cannot be
 11 discriminated against in this context, technology can
 12 enable that to happen anyway, where data could be used
 13 as proxies.
 14 So you may not be able to not hire someone based
 15 on their race, but if you know what type of shampoo they
 16 use based on their online purchasing history or browsing
 17 history, that shampoo could be used as a proxy for race.
 18 So I think with some of these we need to think about
 19 different methods to ensure that we are making sure that
 20 data are not being used as proxies for protected
 21 classes. I think that is a very clear top-level
 22 approach to preventing some of these harms, but ensuring
 23 that -- you know, that is sort of built into how we're
 24 thinking about these issues, writ large, and that there
 25 are technological solutions to some of these, you know,

1 algorithmic designs to consider whether protected status
 2 should be used as an input in certain contexts.
 3 And sometimes it may be helpful to include
 4 protected class status so that it could be checked to
 5 ensure that decisions are not being made based on that,
 6 but it also may be important to consider how it's being
 7 used throughout the process.
 8 And then when you get down to sort of less
 9 crisply defined harms, you know, it's important to think
 10 about -- you know, in some of the conversations
 11 recently, you know, are we calling on tech platforms to
 12 define societal norms? And is that sort of too much to
 13 ask as we're thinking about these issues?
 14 And considering that, you know, for things like
 15 network bubbles and narrowing of choice, we haven't
 16 created a clear set of societal norms yet, but if there
 17 are business processes that are taking these into
 18 account, that are considering the ways in which these
 19 products could have impacts like this, sort of creating
 20 ethical frameworks, creating best practices to monitor
 21 and check for ways in which data in a data set could be
 22 used to have some negative impacts, that that is really
 23 something that should be baked into how we're thinking
 24 about new technologies going forward.
 25 MR. MCCOY: So I think one big area that we have

1 seen in society that's lacking is this online harassment
 2 stuff, right? In the doxes I showed you, it's hard to
 3 point at a law that currently exists that would outlaw
 4 that type of behavior. And as the FTC showed, they had
 5 to kind of creatively go after these revenge porn sites,
 6 and then finally the states are kind of stepping up,
 7 piecemeal, and enacting laws, but there's a huge gap in
 8 terms of understanding, right, the laws defining
 9 nonconsensual posting of people's information online.
 10 MS. DIXON: I would like to focus on one of the
 11 harms that is very, very tied to medical forms of
 12 identity theft, which is very aggressive, unethical, and
 13 often illegal medical debt collection. So individuals
 14 who have written in complaints both to the FTC and the
 15 CFPB have routinely stated that they are working to get
 16 debt collections off of their credit bureau files for
 17 one, two, and three years, and there's narratives
 18 actually in the report we just put out of victims of
 19 medical identity theft who literally cannot buy homes
 20 and cannot move on with their life because they're being
 21 held hostage by debt collectors.
 22 And some of the debt collectors will even tell
 23 them, you know, if you just pay us \$200 on this debt, we
 24 will let you go. It's just a horrifying mechanism. And
 25 I do think it would not be a profoundly expensive item

1 to fix, to really take a closer look at medical
 2 collections and really clean up that niche of a sector.
 3 I think it's an area that causes a lot of harms to a lot
 4 of folks over extended periods of time.
 5 MR. WOOD: Okay. Well, this has been incredibly
 6 interesting, and I think we could go on all day, but we
 7 promised that we would leave some time for audience
 8 questions. So we have two questions from the audience,
 9 and the first one I guess is addressed generally to the
 10 panel. They are both addressed generally to the panel.
 11 So it is, can the panel speak to how to
 12 characterize the lower level of informational harms that
 13 exists and affect day-to-day life but don't rise to the
 14 level that is being discussed by the panel?
 15 Anyone?
 16 MS. DIXON: I wish we could ask a followup
 17 question more about what they meant. You know,
 18 information annoyances beleaguer all of us, and it
 19 really does take some time to figure out, okay, is this
 20 annoying or is this a problem? Some of the doxing and
 21 the spyware, I mean, these are large problems, but they
 22 may start as smaller ones. I think that this is a
 23 difficult question without knowing more from the asker.
 24 I apologize.
 25 MR. MCCOY: And you can clearly point at the

1 target advertisements, things like that, ads that are
2 showing up on people's pages that are clearly revealing
3 other things they are searching, and if people can see
4 their screens, they can quickly infer other things that
5 people are searching that are, you know, sometimes or
6 oftentimes very private.

7 MS. DIXON: You know what, I did think of
8 something that actually I think is a low -- well, not a
9 low level, but it's an everyday informational issue.
10 Most people who call our office are interested in
11 stepping up their privacy game, and one of the first
12 things I ask them is how they're using their financial
13 tools and services, and really, if you want to really
14 see a lot of privacy informational issues that are on a
15 lower level, not necessarily hurting you but just
16 circulating about you, really you have to learn how to,
17 you know, shut down some of the financial data flows.

18 It's easy to do, there's a lot of opt-outs, but I
19 do think that's a general annoyance that kind of filters
20 through all of our lives, you know, unless you, of
21 course, want to pay cash for absolutely everything, and
22 I don't know anyone really who's able to do that
23 anymore, it's just not a very easy way to live.

24 MR. WOOD: Anybody else, or should we move on to
25 the second question?

1 Okay, so the second question is, to what extent
2 are the harms experienced in these events purely due to
3 the actions of a miscreant versus the negligence of a
4 data steward?

5 MS. SOUTHWORTH: I can jump in on this one. I
6 think that is the million dollar question. You know,
7 one of the -- I would say the easy bad actors for me are
8 the ones like Remote Spy that were actually advertising
9 to allow you to spy on anyone from anywhere. That's
10 just an easy lift of, yeah, they're pretty much
11 malintended.

12 I think where it's more challenging is if my
13 information is compromised through a fairly innocuous,
14 minor data breach, does that information identify
15 something about me that then has later long-term impact?
16 You know, do I not get hired because of my history of
17 domestic violence or sexual assault, or whatever stigma
18 it might be, because something that was accidentally
19 leaked and then makes its way through the stratosphere?

20 I mean, I think the blatant bad actors are easy
21 targets for us to point to, but I do think there are
22 unintended consequences of breaches that at least my
23 constituency sort of runs into.

24 MS. SMITH: And I think the reality is that
25 personalization has become a service and something that

1 we are very used to seeing on online platforms and
2 technology devices that we use, and there's a lot of
3 benefit there to consumers, but it also sort of leads to
4 downstream impacts.

5 And so, you know, just as there is more data
6 built on an individual, if that information is used in a
7 way that an individual does not know about and would not
8 prefer, then that could be perceived as a harm to them,
9 and it could have, you know, depending on the type of
10 harm, could have either slight or significant impacts on
11 their lives.

12 Again, I think some of these questions are not
13 settled questions, you know, are -- is having a -- the
14 set of information that is presented to you when you log
15 into an online platform personalized to you based on
16 what your friends like? based on what you've shopped
17 for? That may provide you with a great service that you
18 really enjoy, but it also, you know, could be used in
19 other ways that you may not prefer.

20 And so I think some of these harms we are still
21 just starting to understand, and as much, you know,
22 transparency and control that consumers are able to
23 have, I think the more we're able to sort of safeguard
24 in the long run how they play out.

25 MR. WOOD: Anyone?

1 Well, I guess we have about a minute each for
2 final thoughts from the panelists. Does anybody --
3 should we -- can we just start with Pamela?

4 MS. SOUTHWORTH: I want to just sort of -- not
5 being a legal expert but instead talking about very
6 pragmatic things, I loved the example that Damon used
7 about how technology filtering can make such a
8 difference to somebody's online experience and help
9 mitigate harassment.

10 We've seen very pragmatic approaches to
11 information harms in my 27 years of doing this work.
12 One was a domestic violence shelter years ago that their
13 address was accidentally published by the local phone
14 company, and the phone company paid off their mortgage
15 and helped them move, not a light lift, but very
16 practical and very pragmatic.

17 I think the granular attempts to allow people to
18 control their own experiences, such as filtering
19 comments within Instagram, Facebook, Google is working
20 on it, will help people be able to stay online and have
21 less assault and harassment coming at them.

22 MR. WOOD: Okay. Well, thank you.

23 Other final thoughts?

24 MS. DIXON: I have a comment about solutions.
25 Very often I hear people talking about solutions and,

1 oh, well, we are going to solve our medical identity
2 theft problem by installing a biometric system to make
3 sure all these patients are who they say they are.
4 Meanwhile, they have got a huge security problem in
5 their biometric system.

6 There is not anymore -- it is just not possible
7 to find a single silver bullet, gorgeous, perfectly
8 formed solution that will solve 100 percent of an
9 informational problem. It doesn't exist. We have to
10 look at layers. We have to look at different facets.
11 We have got to have a multifactorial approach to any
12 kind of problem that we're trying to solve.

13 And I really like the idea of collaboration
14 across states and federal agencies. I like the idea of
15 a collaboration among different expertises and against
16 different types of victims and a variety of
17 stakeholders. I think it's an important approach, it
18 gets a lot of ideas on the table, and it avoids the
19 dangers of the quick, easy solution.

20 I always like to say that the absolute longest
21 shortcut or the absolute longest distance in the world
22 is a shortcut. You have got to take the time to find
23 the nuances in the solution or it's just going to be a
24 disaster.

25 MR. MCCOY: So I will echo what Pamela said, is

1 that I think we really do have to put a lot of effort
2 into trying to understand and measure the kinds of harms
3 that are going on and get a good grasp on these
4 measurements, because when we start deploying solutions,
5 it's going to be impossible for us to say whether the
6 solution actually helped or potentially harmed people
7 unless we have these good, deep measurements of the
8 kinds of harms and the scope of the harms that we're
9 dealing with.

10 MS. WYDRA: And I will make a final remark. You
11 know, I have been actually impressed by the discussion
12 here and its mix of technology, but also of compassion,
13 and it's not necessarily what I would have expected from
14 a panel talking about or at the FTC talking about these
15 types of things, especially that a lot are
16 computer-based and technology-based, but I think that's
17 been a part of everything that we have all talked about.

18 Of course, we want these types of data breaches
19 and personal information to be protected, but when it
20 isn't, it has to be dealt with with compassion, and it's
21 important to understand, as you just said, the types of
22 harms that happen, because it makes people more
23 motivated to make sure that they don't happen.

24 MS. SMITH: And I would say as we think about
25 these injuries, writ large, to ensure that we are sort

1 of approaching them methodically and really identifying
2 the harms that we're most concerned about and separating
3 that from sort of what the causes might be and using
4 that as a step to get to what the solutions might be,
5 and then understanding that technology in its many forms
6 today can create some of these harms but could also be
7 used as a tool to prevent some of these harms that may
8 have been perpetuated by sort of humans in a less
9 technological form before but now could potentially be
10 mitigated with these technologies.

11 MR. WOOD: Okay. Well, that's nice to end on a
12 hopeful note, but we do have to end. So there will be a
13 30-minute break after this panel, and so the next panel
14 begins at 11:15. The cafeteria is open until 11:00, so
15 if you --

16 MS. CONNOR: Not it's -- oh, open until 11:00,
17 I'm sorry.

18 MR. WOOD: Open until 11:00, and then it closes.
19 So if you want coffee, that is your best bet. We will
20 see you back at 11:15.

21 (Applause.)
22 (A brief recess was taken.)
23
24
25

1 PANEL 2: POTENTIAL FACTORS IN ASSESSING INJURY

2 MS. MITHAL: My name is Maneesha Mithal, and I'm
3 the Associate Director of the Division of Privacy and
4 Identity Protection, and with me is my co-moderator,
5 Neil Chilson, who is the Acting Chief Technologist of
6 the FTC.

7 I want to introduce the panelists quickly. Their
8 bios are in your packet, so I won't go into detail. We
9 have Alessandro Acquisti from Carnegie Mellon; James
10 Cooper from George Mason; Michelle De Mooy from the
11 Center for Democracy and Technology; Geoffrey Manne,
12 from the International Center for Law and Economics; and
13 Paul Ohm from Georgetown University.

14 So before we get started on this panel, we just
15 want to set the stage a little bit. Now, on the first
16 panel, you heard a lot about the bad outcomes, the
17 really bad outcomes that can come when bad actors, in
18 particular, get your data, and in this panel we are
19 going to be talking a little bit more about the
20 responsibilities of commercial entities that collect and
21 store your data.

22 And so what we are going to be doing is we are
23 going to present a privacy hypothetical and a security
24 hypothetical, and we're going to ask the panelists to
25 raise their hands in the hypotheticals when they hear

1 that there has been injury taking place. And the goal
 2 is not to come to any legal conclusions but to really
 3 have a policy discussion and a policy back-and-forth
 4 about why people raised their hands when they did.
 5 We also want to ask the panelists if you could
 6 raise your name tents when you have something to say so
 7 we know who to call on. We do hope that there is some
 8 really interesting back-and-forth. And Neil and I will
 9 be switching off moderating duties, so with that, let me
 10 just turn it over to Neil.
 11 MR. CHILSON: Thank you very much, Maneesha.
 12 Thanks to our panelists for being here. And thanks to
 13 all of you.
 14 So, yes, so we are going to do a hypothetical
 15 here, and when -- the panelists, as I read this along --
 16 and there will be accompanying bullets on the screen for
 17 the audience. Once you raise your hand, unless you hear
 18 something that changes your mind about whether there's
 19 been consumer injury, leave your hand up. And then,
 20 like Maneesha said, we will be discussing why you
 21 identified injury at that particular point.
 22 So with that, on to our privacy hypo. So in this
 23 hypothetical --
 24 MS. MITHAL: I'm sorry, while we are getting the
 25 technology cued up, I just want to give one disclaimer,

1 which is that we're really not here to talk about the
 2 law and the kind of legal ramifications of Section 5.
 3 We are really here to talk about injury as a policy
 4 matter. So, again, when people raise their hands, this
 5 is not kind of what qualifies as injury under Section 5,
 6 but this is kind of when do you think injury has
 7 occurred.
 8 MR. CHILSON: And part of this is to explore less
 9 the line that the participants have drawn in raising
 10 their hand and more why they decided at that point to
 11 raise their hand. So on to the privacy hypo. (Slide 21)
 12 A pharmacy uses retail tracking in its stores to
 13 determine the most effective way to display greeting
 14 cards. (Acquisti, De Mooy and Ohm raise hands.)
 15 The pharmacy then begins to track aggregate
 16 consumer interest in over-the-counter HIV tests.
 17 The pharmacy begins selling this aggregate
 18 information to interested market analysts.
 19 One marketing company uses its own algorithm to
 20 associate this aggregate information with other data to
 21 estimate the probability that a specific consumer has
 22 purchased either a greeting card or an HIV test.
 23 (Cooper raises hand.)
 24 The marketing company then uses the data to
 25 target advertising to identified consumers, including

1 Carl Consumer. (Cooper lowers hand.)
 2 Now, continuing with the HIV test example, the
 3 marketing company advertises HIV tests to friends and
 4 associates in Carl Consumer's social network.
 5 MS. MITHAL: James, is your hand up or down?
 6 MR. COOPER: It was up and now it's down -- it's
 7 resting. I am very weak.
 8 MR. CHILSON: The ads mention that Carl Consumer
 9 recently purchased this product. (Cooper and Manne
 10 raise hands.)
 11 A local insurance company gets this information
 12 and raises rates for Carl Consumer. (Cooper lowers
 13 hand.)
 14 Carl Consumer's employer sees one of the ads and
 15 fires Carl.
 16 So those are the eight sort of framing sentences
 17 of the hypothetical. We got an early jump there, and I
 18 am very curious about what that is. I think --
 19 MR. COOPER: Before you even said anything.
 20 MR. CHILSON: Yeah, and I'm very curious about
 21 why that is and what it was in that first sentence -- I
 22 have some suspicion that "retail tracking," as a term,
 23 has some baggage, and so let's just kind of run down the
 24 line here and have each of you explain why you raised
 25 your hand when you did, starting with Alessandro.

1 MR. ACQUISTI: Well, this is my thinking.
 2 Clearly, if you are defining injury or harm specifically
 3 as a realized and a quantified economic harm, I suppose
 4 that most of us here and the ones who raised their hands
 5 in the first scenario there would agree that there was
 6 no realized quantifiable economic harm.
 7 However, there would be a very reductionist
 8 definition of injury which would ignore scholarly
 9 research on privacy, not coming from the legal
 10 profession that I know you want to avoid for this panel,
 11 but coming from social sciences.
 12 Think about the work by Irwin Altman, for
 13 instance. Privacy is not the protection of data.
 14 Privacy is a dialectic process of boundary management,
 15 which includes both the opening of the self to others
 16 and the closing of the self to others. These boundaries
 17 are affected by social norms, expectations, individual
 18 preferences.
 19 So in the context you are bringing up in the very
 20 first -- with the very first scenario, some of the key
 21 questions for me would be whether Carl was, indeed,
 22 aware that, as he was walking through the store, his
 23 behaviors would be tracked. Did he consent to this
 24 information being used for other purposes? If not, then
 25 there is a possibility that that boundary has been

1 broken, and when the boundary has been broken, well,
 2 then, that can be considered an injury.
 3 In addition, I can easily jump from scenario one
 4 to scenario nine, which is the -- perhaps the most of
 5 the actual realized harm by creating a slightly
 6 different hypothetical, which is the pharmacy is using
 7 tracking via video. The video gets leaked. Carl's
 8 employer sees the video with Carl and fires Carl.
 9 So we jumped entirely the other eight steps --
 10 seven steps, and we went directly to the harm. So the
 11 point being here that when there is a breakage of the
 12 boundary, we increase the likelihood of a potential
 13 downstream cost, what economists refer to as expected
 14 costs, which are very important to consider, because
 15 agents, economic agents, both consumers and companies,
 16 make decisions based on expected benefits and expected
 17 costs. So we have to consider that in analyzing privacy
 18 harm.
 19 Finally, I tend to steer away from a purely
 20 narrowly economic definition of injury and harm because
 21 the harm itself, the economic harm, even when it's
 22 there, it's incredibly hard to quantify, and for a
 23 number of technical reasons, which I hope I can -- we
 24 can get into later. I probably can pause here, let
 25 others talk, but I would like to go back to the issue of

1 why quantifying economic harm is so hard.
 2 MR. CHILSON: Great.
 3 James?
 4 MR. COOPER: Yeah, thanks, and thanks for
 5 inviting me. It's great to be here.
 6 So I get -- you know, I raised my hand -- I kind
 7 of went up and down a lot, and so one -- one, two, and
 8 three, you know, we still have that aggregate as the --
 9 as the qualifier there. So you think that I have
 10 something private that I want to control the
 11 information, so if this is aggregated and there's no --
 12 it is not really known, I'm not -- nothing has been
 13 revealed about me.
 14 So, you know, in -- and you can even -- and I'm
 15 willing to even entertain the notion that you may want
 16 to keep your interest in greeting cards private. I
 17 mean, no -- I'm not here to dispute -- this isn't about,
 18 you know, well, that's obviously innocuous, who cares?
 19 I mean, someone could genuinely have utility loss from
 20 having people see the greeting cards they're looking at
 21 or something like that. But at this point, no
 22 individual person knows, certainly no algorithm knows
 23 about you.
 24 When you get to number four, I think it gets --
 25 and I put my hand up here -- and I think it gets to be a

1 closer call because at that point you're taking this
 2 aggregated information and somebody's saying, okay,
 3 well, now I want to find out more about Carl. I want to
 4 pull out -- I've got this giant lump of data, of people
 5 who have been at this drugstore, but now I want to see,
 6 what's Carl into? What is he buying?
 7 And at that point you're starting to reveal
 8 something about Carl, and so I think there you start to
 9 get into -- if we're talking about privacy harms or
 10 informational injury, I mean, if we're thinking about
 11 the kind of harms that can involve privacy -- and I
 12 think I can talk about a distinction there in a
 13 minute -- that at this point you could have that because
 14 something is being revealed specifically about Carl.
 15 So to me, one of the big differences between --
 16 you know, just to sum up -- you know, between one
 17 through three and then four is you're going from
 18 aggregate to individualized, and then you think that's
 19 where you can get into the dignitary harms, the things
 20 that we think about with privacy.
 21 Now, when we get into number five, at that point,
 22 the -- you're -- and I guess it was maybe unclear what
 23 the hypo -- this is the kind of thing where my student
 24 would come to me saying, I don't understand, it wasn't
 25 clear, and that's why I missed it.

1 MR. CHILSON: There's no right or wrong answers
 2 here.
 3 MR. COOPER: Yeah. Well, there are on my finals.
 4 MR. CHILSON: There might be later on.
 5 MR. COOPER: Yes. So, anyway, the -- here, you
 6 know, there are two potential harms. So the -- you
 7 know, you're targeting ads to customers for this -- and
 8 it didn't really say are you targeting ads for greeting
 9 cards or HIV tests? And here I think that -- now, with
 10 the greeting cards, maybe there's not a harm with the
 11 HIV test. I still think it's a targeted ad. You're not
 12 really -- you do have the potential cascade where
 13 someone's looking over your shoulder or sees that you
 14 get an ad for an HIV test.
 15 Well, what does that mean? Kind of like the
 16 Target baby ad thing that people talk a lot about, but I
 17 have a harder time with, you know, targeted ads in
 18 general. I mean, it's kind of an intrusion into
 19 seclusion maybe, but I have a harder time there.
 20 And the same thing with, you know, number six.
 21 Here it's like, okay, I've got this data, and it seems
 22 that Carl's interested in these HIV tests, and so Carl's
 23 got a network of friends, and I'll advertise it to
 24 those. And, again, as long as they're not necessarily
 25 linking that -- you know, maybe somebody's light bulb

1 goes off and says, oh, I'm getting this because I'm
 2 friends with Carl.
 3 I think that's a tenuous -- maybe too tenuous of
 4 a link, but my hand then goes up, of course, when we get
 5 to number seven. I think there that that's clearly a
 6 privacy harm at that point, because you're revealing
 7 something about Carl. And, again, part of the hypo here
 8 is we don't even know if it's true or not, but
 9 regardless, you know, you have made a prediction that
 10 Carl is purchasing these HIV tests, and all the -- and
 11 it's certainly something very sensitive, and you're
 12 telling all of his friends in his network, you know say,
 13 "Hey, buy this, because Carl has bought that."
 14 And I think at that point you're revealing
 15 something sensitive to people, and I think that there is
 16 some -- you know, there's some empirical lit out there
 17 to suggest that people care more about revelation to
 18 other people than they necessarily care about an
 19 algorithm or a server somewhere, you know, knowing
 20 something about you.
 21 Now, finally, and, you know, when we get to
 22 eight and nine, this is where I kind of make a
 23 distinction between -- I think there are two things you
 24 have to think about. There's the direct disutility harm
 25 that comes from someone knowing something private about

1 you. I have written about this a little bit, I call it
 2 intrinsic privacy harm, but essentially that dignitary
 3 harms, loss of autonomy, all of the sort of truly -- the
 4 loss that you feel when someone knows something private
 5 about you or you lose control of your information.
 6 Now, the out -- then there's the -- the outcome
 7 that when a third party knows that about you, they act
 8 on that information. Now, if it's -- and I know this is
 9 maybe something we will get into a little later. I
 10 mean, maybe it matters if it's true or not, but assume
 11 for now it's true. If the insurance company now knows
 12 something true about Carl and makes a decision based on
 13 that, now Carl would like to keep that secret, I mean,
 14 that's strategic on his part, like I would like to pay a
 15 lower insurance rate, and the insurance company now
 16 knows that.
 17 Now, that's -- is that -- it's a consumer harm to
 18 Carl, yes, he's paying higher insurance rates, but
 19 just -- you know, it's a reduction in adverse selection.
 20 So in some ways the surplus for society as a whole is
 21 getting larger. Now, I know this sounds cold-hearted,
 22 I'm not saying, "Oh, you know, poor Carl," but it's not
 23 to say -- and then, you know, going further, I'll lump
 24 the boss in there, too. So the boss fires him.
 25 Now, there are a million reasons the boss may do

1 that, legitimate, illegitimate reasons, and that -- but,
 2 again, if they're acting on truthful information, then
 3 I -- but I wouldn't categorize that as a privacy harm.
 4 I mean, there are very legitimate reasons why we as a
 5 society prevent classification on certain -- based on
 6 certain attributes, but those are third parties acting
 7 on truthful information, and I think that's not the same
 8 as a dignitary-type harm that comes from privacy.
 9 And I think you should make a -- there's a
 10 distinction in that -- again, we can use discrimination
 11 law to get at these, we can use other means, and this
 12 isn't -- this panel is not about law, but I think that
 13 there are -- to me, in my mind, there's a distinction
 14 between those two.
 15 And I've probably gone on too long, but...
 16 MR. CHILSON: No, that's fine.
 17 Michelle?
 18 MS. DE MOOY: Everyone, thank you so much for
 19 having me.
 20 So where I'm starting is with the idea of privacy
 21 as a core principle to democracies, in particular. And
 22 so when you start with that, the reason that I raised my
 23 hand at the very first part of the hypothetical, which I
 24 knew would be kind of funny in a sense, it's not that I
 25 think that this person has been injured in a physical

1 way, per se, but I do believe that the violation of
 2 privacy has occurred, and the reason is because, first
 3 of all, their expectations matter.
 4 So when you walk into a pharmacy, I think most of
 5 us -- or any kind of store -- don't have the expectation
 6 that our phones will be pinged repeatedly by a tracking
 7 system. Also, the idea of whether or not Carl was asked
 8 for consent, did he -- was he asked for permission to
 9 ping his phone? And, of course, when that happens, it's
 10 typically not just one small piece of data that's
 11 getting extracted, but many. So had he given his
 12 permission for that to happen? Did he have any control
 13 over the level of tracking that occurred? In other
 14 words, did it every single time he went into the store
 15 happen or just this one time for 15 minutes or when he
 16 was near the greeting card area?
 17 Also, what was the benefit to Carl in this
 18 scenario? I think this is something I want to bring up
 19 later, because I think it's hugely important here. You
 20 know, a lot of the discussion around privacy, and
 21 particularly I think in FTC cases, sort of assumes that
 22 there's a benefit to consumers, to individuals,
 23 through whether it's behavioral advertising or tracking
 24 of any kind. And I think the question to ask is, where
 25 was the benefit here? Did he receive any kind of

1 benefit for this transaction?
 2 Also, did he have access to or understanding
 3 awareness of what was occurring? This goes along with
 4 expectations and consents. And then also the idea of
 5 risk I think should come into play. So we know that the
 6 way that privacy harm happens is through small privacy
 7 violations perhaps, right? And I think this was
 8 discussed a little bit on the last panel. It begins
 9 small.
 10 And so, therefore, the very first part of
 11 collection and tracking, that is where the risk is
 12 raised. So the fact that this information, what was
 13 taken without permission, et cetera, which is my
 14 assumption here, that means that his risk for
 15 identification, his risk for all of the other harms that
 16 come later has been elevated, and so that triggers
 17 obligations of the tracking company in terms of whether
 18 or not they are providing benefit, whether they're
 19 providing control and access.
 20 And then I would -- you know, my hand would be
 21 raised for the rest of them, of course, but for
 22 different reasons; similar sort of principles but
 23 different reasons. For example, the aggregate to me is
 24 meaningless. The fact that it's aggregated is -- you
 25 know, it's one method, but it's very meaningless when it

1 comes to protecting information and protecting it from
 2 identification.
 3 For example, how much data was there in this
 4 collection? Maybe there was three people who bought an
 5 HIV test, and, therefore, you know, Carl is pretty
 6 exposed in that aggregate data set. So, you know, it's
 7 not clear there, but I would say that aggregation, in
 8 and of itself, is not a panacea to any of these other
 9 issues.
 10 And then the idea that this is also related to
 11 health information, you know, I don't think that
 12 sensitivity of data is everything by any means, but I do
 13 think when you're talking about health information, and
 14 particularly highly sensitive health information, like
 15 HIV status or a concern about HIV status, that elevates
 16 it, because this is immutable information, right?
 17 Our health is not information we can replace
 18 easily. It's not information that can go somewhere
 19 else. It is immutable and intrinsic and inherent to us.
 20 And so, therefore, I think it raises more risk in terms
 21 of harm.
 22 I think, finally, the idea of whether or not a
 23 person has recourse or -- you know, this ties to
 24 awareness and consent and expectation, but do you have
 25 any means to change this or to say I don't want this

1 information to be marketed or I -- you know, I don't
 2 feel like this is in my best interest and, therefore, I
 3 would like to reduce my risk of some of the harms that I
 4 see occurring by not allowing this collection to happen
 5 in the first place?
 6 MR. CHILSON: Great.
 7 Geoff?
 8 MR. MANNE: Thanks, Neil, and thank you for
 9 having me here and thanks for listening to us
 10 pontificate, as if we know something.
 11 That is a big part of what I want to say here, is
 12 that there's a lot less that we know than that we don't
 13 know in this area, and one of the really crucial things
 14 that I have been sort of thinking as I have been
 15 listening to people talk is that people are identifying
 16 something as injury, but they are not the sorts of
 17 things that we would all clearly understand as injury,
 18 in ways that are -- it's just not clearly the case that
 19 those things are, in fact, injuries, that they harm
 20 utility, that they are a painful or otherwise
 21 objectionable thing to, let's say, most people. Even
 22 that is hard to know what the right categorization is.
 23 And so, you know, so one of the things here is
 24 that all of the things that we've been talking about and
 25 all of the things on the hypotheticals are all

1 describing aspects of information relationships. They
 2 are talking about how various entities interact with
 3 consumers around information, but that isn't the same
 4 thing as an injury.
 5 The fact that information may be involved in
 6 something that's happening and has probably happened in
 7 some form or another since the beginning of time doesn't
 8 convert it into an injury. It helps to describe it, and
 9 it may help to understand how it could lead to injury.
 10 It may help us in certain contexts to understand things
 11 that are, in fact, injuries, and this goes back to my
 12 first point. We don't know that yet, but with enough
 13 data and enough analysis, maybe we can figure that out.
 14 And so I -- all the way up until at least number
 15 seven, my sense here is that anyone who says that
 16 there's an injury here is either generalizing from their
 17 own experience, which is really all we can do, but
 18 still, we need to be very cautious about that, or
 19 intentionally or not converting an information
 20 relationship into an information injury, and I want to
 21 caution very strongly against that.
 22 I think that risk is, of course, a really
 23 important part of this, but a risk of an injury is not
 24 actually an injury, and that's another really important
 25 piece here. For example, with number six, the marketing

1 company advertises HIV tests to friends and associates
 2 in Carl Consumer's social network, let's say -- I don't
 3 actually know for certain that this is true -- but let's
 4 say that it's fairly clearly the case that Carl would be
 5 injured if the information about the HIV test were
 6 revealed to people who could identify him, right, to
 7 people he knows or something.

8 The fact that the -- the marketing the test to
 9 friends and associates in Carl Consumer's social
 10 network -- and I'm assuming someone named Carl Consumer
 11 is going to have lots of friends, so it is not going to
 12 be clear that it's him -- but that may indeed increase
 13 the risk that someone will be able to figure out that he
 14 had purchased an HIV test, and that may, indeed, impose
 15 harm, but that fact itself does not strike me as
 16 anything that we should recognize as itself being an
 17 injury.

18 If risk of injury were enough to constitute
 19 injury, literally everything, literally the existence of
 20 these businesses would increase the risk of injury and,
 21 therefore, be actionable. And I think we would all
 22 understand that that can't possibly be the case.

23 I think it's also difficult in the context of how
 24 the panel was set up, but it's difficult to talk about
 25 injury without also talking about countervailing

1 benefits and talking, therefore, about sort of net
 2 injury, right? James started to talk about this a
 3 little bit, and I don't know -- you know, maybe we
 4 should be more clear about this as we go ahead. It may
 5 be that, for example, with the revelation that Carl
 6 bought an HIV test, that Carl himself was injured. It
 7 may also be that all of Carl's sexual partners now know
 8 that they should go out and buy an HIV test themselves,
 9 and the net benefit may be quite positive. That's also
 10 the case, as James pointed out, with respect to the
 11 insurance company, but I think particularly acute in
 12 that instance of Carl's social network knowing that Carl
 13 bought an HIV test.

14 Now, again, obviously -- I think, again, with the
 15 caveat that none of us really knows -- but let's say
 16 obviously it's a harm to Carl, but is it an injury that
 17 we really want to stop? Is the conveyance of
 18 information that could lead to net social benefit
 19 something that we should be calling a harm?

20 I think we have to be a little -- you know, sort
 21 of careful about that, but, again, just -- it's
 22 important in this context to caveat that. I understand
 23 why it's a harm to Carl, but the relevant question here
 24 is, is it a harm that the FTC, for example, should take
 25 account of? And that's a little bit harder.

1 MR. CHILSON: Great.
 2 Paul?

3 MR. OHM: So all four of the co- panelists did
 4 such a great job kind of dealing with this, so I am
 5 going to spend most of time now responding to things
 6 that have been put on the table.

7 Nobody I think, if I recall, tried to kind of
 8 define what they mean by "harm" just to begin, so one
 9 working definition that I think philosophers and legal
 10 scholars have used is, are you worse off than if the
 11 conduct had not occurred, right?

12 And I think that, frankly, the liberating conceit
 13 of that we're not supposed to think about the law, we
 14 are just supposed to think about the word "harm" and
 15 "injury," makes these hypotheticals really easy, in ways
 16 that I think Alessandro and Michelle pointed out, that
 17 in almost every -- in every single one of these, we can
 18 point to something that is an injury.

19 Now, I think a lot of Geoff's comments portrayed
 20 the idea that they may not be injuries that we want the
 21 legal system and the legal apparatus in an enforcement
 22 agency to be able to remedy, but that's a different
 23 question than the question of has an injury occurred.
 24 So let me just address some of the things that were
 25 said.

1 One is risk of injury is not an injury. That
 2 makes absolutely no sense to me, right? We have many
 3 examples economically, but also, if we take a broader
 4 lens on things, where if something is in state one and
 5 then, because of the action of another, it becomes a
 6 much riskier state two, you have been injured, right?

7 We do this in medical malpractice contexts. We
 8 do this when it comes to the value of our consumer
 9 goods. If you didn't face a risk, and because of the
 10 action or negligence of another actor, you now face that
 11 risk, that's an injury. I don't even understand how it
 12 is not, and that's kind of in broad economic terms.

13 Layer on top of that, in the way that Alessandro
 14 urged us to, a hundred years of writing about emotional
 15 distress and anxiety, the kind of things that befall
 16 every one of us given the information insecurity we all
 17 live in, and I know this is the privacy question, but it
 18 goes for privacy as well, right?

19 I mean, if any of you were you in the room for
 20 the first panel, I bet your pulse started to quicken
 21 about midway through and probably hasn't come down yet,
 22 right? Knowing about the harms that we are all
 23 subjected to -- and, again, there might be
 24 countervailing benefits that justify these harms -- but
 25 knowing that there's an increased risk of certain harm

1 is itself an injury, and I say that kind of both from
 2 this abstracted, philosophical conversation, but I'm
 3 happy to say that as we move into thinking about the law
 4 later.

5 Let me say two more quick things. James put on
 6 the table and I think Michelle capably rebutted the idea
 7 that the word "aggregation" is some sort of kind of holy
 8 shield that can protect you from the idea that you're
 9 putting at risk the people whose information you are
 10 handling.

11 Now, the one thing that I've said in a lot of my
 12 writing and I think is pretty intuitively understood now
 13 is that utility of information of the kind Geoff was
 14 talking about is the other side of the coin of privacy
 15 invasion, that if you aggregate the data so much that
 16 you're reducing the risk of privacy harm to almost zero,
 17 you've also rendered that data totally unuseful for any
 18 commercial purpose.

19 On the other hand, if what you mean by
 20 "aggregate" is, yeah, it's aggregate. We don't know
 21 your name, but there is so much rich information about
 22 your transaction or the transactions of a few people
 23 that we are going to be able to, like, sell it to
 24 advertisers and insurers and employers, then that also
 25 means that the risk of privacy is still latent within

1 there, and so you can't have one without the other,
 2 right?

3 I wish there were a magical wand that we could
 4 wave that would suck out all the privacy risk from a
 5 pool of data and yet retain the utility. That doesn't
 6 exist. It's the exact same attribute of data that
 7 provides both of those things.

8 Last, but not least, when I read the first
 9 hypothetical, I thought, what is a retail store? And
 10 then I remembered these past memories from my childhood
 11 where you would walk into these buildings and buy
 12 things. One thing I think we should think about when we
 13 think about privacy and harm is what kind of population
 14 is affected by the harm, right?

15 And I think it's fair to say that for certain
 16 retail establishments today, we're talking about an
 17 older population, a less digitally connected population,
 18 maybe a less educated population. I think that's fair
 19 game to bring into our harm analysis as well, that if
 20 there's a harm that maybe isn't visited on most of us
 21 because we all are Amazon Prime customers at this time,
 22 but it is targeted at, you know, older people who go to
 23 a particular pharmacy, I think that should factor into
 24 the way we assess the harm.

25 Thanks.

1 MS. MITHAL: So there is a lot to unpack here,
 2 and, Geoff, I will give you a chance to respond, but let
 3 me just tee up the question I think everybody wants to
 4 talk about, which is, okay, you have all raised your
 5 hands and identified where you think there's a harm.
 6 Now, at what point do you think there should be
 7 government intervention?

8 And so maybe we can start with Geoff and go back
 9 down -- or actually, why don't we start on the other
 10 side. We will start with Paul and come back down this
 11 way, and maybe just tell us the number of where you
 12 think that there should be government intervention.

13 MR. MANNE: Can I just respond to one thing Paul
 14 said first before we do that that I think will help,
 15 because it's not about that?

16 MS. MITHAL: Sure.

17 MR. MANNE: I do want to just sort of reiterate
 18 what I said a minute ago, Paul, and try to hear more
 19 about how a risk of harm can itself be harm when, again,
 20 literally every bit of activity increases the risk of
 21 injury, right?

22 I mean, that's like saying a drugstore that
 23 serves one additional customer has created a cognizable
 24 injury, because by increasing the amount of activity,
 25 it's also increased the risk that somebody would be

1 injured by whatever might happen -- befall that
 2 drugstore. So I don't think it can be that.

3 I also think that it's essential in trying -- I
 4 like that Paul actually tried to identify a little bit
 5 the kind of disutility that one could experience from
 6 even a risk of harm, this sort of idea that the
 7 knowledge of risk can create an anxiety. And I'll admit
 8 that that could very plausibly be an actual injury, but
 9 then I get back to my very initial point, which is, you
 10 know, we can speculate about that all we want, but I
 11 don't think that makes it so.

12 And I think it behooves the FTC and many others
 13 to try to figure out whether there is actually something
 14 cognizable there, you know, obviously within the context
 15 of the legal regime, but, I mean, even just
 16 independently in terms of defining what injury is.

17 And then, finally, I don't see how any of those
 18 things could be injury if the information is already
 19 known or is already out there or the risk of it being
 20 exposed is already there, so the anxiety is already
 21 there.

22 So one of the really important things here, it
 23 seems to me, from the way I hear a lot of the panelists
 24 talking about it, requires some awareness of the
 25 preexisting risk, in the case of risk, or the

1 preexisting exposure of information, if that's itself
2 going to create a harm.

3 I look, for example, at number two, the pharmacy
4 begins to track aggregate consumer interest in HIV
5 tests. Well, Carl certainly knows that the drugstore
6 already knows if he bought a test. They have that
7 information about him. Whether they're tracking other
8 people's information or not doesn't actually affect the
9 anxiety he might feel about somebody knowing this,
10 because he already knows perfectly well that the person
11 at issue here knows it. So it's hard for me to see how
12 that could increase the risk, at least to Carl, although
13 I understand you may think the aggregation of
14 information creates a second risk, okay?

15 MR. OHM: So I am happy to jump into this second
16 question, and my overly lawyerly answer is, depending on
17 what some of the words mean in the hypotheticals, I
18 think every one of them could justify government
19 intervention.

20 And as part of the backdrop, when I think of
21 government intervention, I think more broadly about
22 legal recourse. Is there a court, under any theory of
23 law, with any plaintiff, that can get recourse for
24 significant injury, right? I want to make sure we're
25 only talking about significant injury.

1 The courthouse doors are being closed to kind of
2 tort plaintiffs left and right, mostly because judges
3 fear that if they allow too many class actions to
4 proceed, it's going to get out of hand and there's going
5 to be a lot of vexatious litigation.

6 So in that climate where none of these things are
7 going to be easily redressable in tort -- or maybe most
8 of them won't be -- I think that kind of raises the
9 urgency for an agency like the FTC to step in,
10 especially when they think there is a serious harm
11 befalling a lot of consumers based on information
12 imbalances. So I think it behooves the FTC to kind of
13 step up and fill the gap of the closed courthouse doors
14 that I'm referring to.

15 And so let me just, you know, go through two
16 really quickly. HIV, right? HIV is not only a kind of
17 significant medical condition that still today, sadly,
18 has a lot of unfounded stigma attached to it, a
19 devastating effect on reputation as we heard in the
20 first panel, but it's also tied intimately to sexual
21 behavior, right?

22 And so to kind of address Geoff's direct point,
23 the hypothetical says interest in HIV, not purchase of
24 HIV, and I take this to mean, you know, perhaps one of
25 these new in-store retail scanners that will tell that

1 you lingered by the HIV test shelf for a while, or maybe
2 if you tie in RFID, that you picked up two of the boxes
3 and then put them back, right?

4 And so to me that's where we're starting to kind
5 of tread into significant sensitive information, and
6 Michelle kind of said that's not the be-all, end-all. I
7 think it's a really useful rubric. I think it's a
8 widely accepted thing outside of the context of the FTC
9 in the law, that we should identify as kind of shorthand
10 aspects of information that are sensitive, and if that's
11 the kind of thing we're talking about, collection in an
12 unexpected or new way or using a technologically new
13 ability, that's where we should be much more worried
14 about the kind of risk of injury that is, in my mind,
15 harm. So that's one line. If you want a line, one line
16 is if information is sensitive, then maybe the
17 government ought to intervene, okay? So that's number
18 one.

19 Let me give you one more. We think a lot about
20 kind of the violation of some other positive law, right,
21 some expression by Congress or by a legislature that
22 some act is not only unexpected in the way Michelle
23 described but also violates some law, arguably violates
24 some law.

25 I think it's become common for retailers and

1 stores to kind of look at MAC addresses emanating from
2 smart phones. I know there has been some activity about
3 this in the FTC. That is an easy violation of the Pen
4 Register and Trap and Trace Act, right? Congress, in
5 its infinite wisdom, has said that this is a misdemeanor
6 crime.

7 Now, there is no plaintiff's action attached to
8 that, so you never see this enforced by anyone, but
9 Congress said, in the same way they did with wiretap
10 law, that there's something about this collection of
11 this kind of information that is illegal, right?

12 So that's a second heuristic, rubric, call it
13 what you want, that would say that the FTC, or some
14 other mythical government agency, should exercise its
15 ability to kind of vindicate the rights of people who
16 are injured in hypothetical one, hypothetical two, and
17 then most of the other hypotheticals flow from one and
18 two.

19 MS. MITHAL: Geoff?

20 MR. MANNE: Okay. So just very quickly, I think
21 one of the things that Paul said and that is sort of at
22 issue in this hypothetical with the retail tracking sort
23 of idea is that when you have a new technology or a new
24 form of data collection, that's where we should be the
25 most vigilant. I think exactly the opposite is true, of

1 course.

2 I think, or at least I think it's imperative to

3 point out, that it is in the cases of newer technologies

4 and innovations that we want to be the most careful

5 about overenforcing the law and overdetering investment

6 in innovation.

7 And so, you know, one of the big problems I see

8 with overenforcement is overdeterrence of

9 experimentation in the sorts of areas that we actually

10 really want, and I don't just mean experimentation with

11 new technologies, but I also mean experimentation with

12 new forms of information relationships that people may

13 or may not actually care about.

14 They may -- that they may actually prefer, that

15 they may be willing to pay for, any sort of number of

16 relationships that you can describe. And if every

17 single effort at trying one of those out leads to

18 potential liability, none of them will ever be tried

19 out. And so that strikes me as being, again, exactly

20 backward.

21 I see also sort of a related reason, a really

22 serious problem, where we're making illegal the

23 collection of data. There should be a really, I think,

24 significant distinction between the collection of data

25 and the use of data; the -- even the increased risk of

1 some actual cognizable harm via a data security problem

2 arising from the collection of data. I think that's

3 really problematic, but at least that has a logical

4 coherence to it.

5 But, again, the idea that by collecting data,

6 we're going to over -- to dramatically deter that, we

7 are never going to find out all of the things that we

8 could do if that becomes the sort of thing that no one

9 actually wants to engage in.

10 And so in terms of trying to identify where the

11 government should get involved, I do think that we

12 should err on the side of, you know, where we actually

13 can really identify that there are viable harms here.

14 Again, in some cases, we are going to know where

15 that is. In some cases, we don't, and that means that

16 before the FTC should start intervening, it should start

17 collecting data. It should start with things like this

18 workshop -- which is great, this is a great start -- but

19 I think there's, you know, years of work to do beyond

20 this before we're going to start -- before we should

21 start identifying that the government should be

22 deterring these examples of data collection.

23 MS. MITHAL: Okay.

24 Michelle?

25 MS. DE MOOY: I just want to push back on one

1 thing that you said earlier, that there's a relationship

2 here, and I think that that's debatable, and in most

3 cases, I think it's debatable whether -- usually a

4 relationship involves at least two parties, and I'm not

5 sure that Carl is aware that he is in a relationship

6 here, right? Maybe it's a stalking relationship, I

7 don't know.

8 So I think that that's an important point to

9 make, you know, that the -- his expectations, his

10 understanding of the situation is probably different

11 from the tracking at the pharmacy and the continued

12 other interests involved here.

13 And part of the reason I bring that up is

14 because, again, the question of whether or not he

15 benefits from this exchange I think should be a part of

16 any kind of legal rubric to determine where -- you know,

17 the level of risk, and I think also, of course, ties to

18 consent and the person's expectation.

19 I think the idea -- you know, the government

20 already intervenes when it comes to sensitive

21 information, so I agree with Paul that sensitive

22 information should trigger obligations. You know, this

23 data, in particular, is not, of course, covered by legal

24 frameworks, but in my opinion should be, not because it

25 should be illegal, but because it should be a part of

1 the assessment for -- whether it's the government saying

2 you're not allowed to do this, and the levels that reach

3 up to that.

4 And then there's the other threshold of maybe

5 harm where there's remedy for the individual, right? I

6 think those are maybe better ways to think about how

7 government intervention would make sense, and this is

8 something that you can see in other frameworks, where it

9 does make sense.

10 I think I fall on the side of collection

11 increasing risk because there is, of course, always the

12 risk of surveillance. This is a fact in our data-driven

13 world, and it is a part of almost every product and

14 service that an individual interacts with in the digital

15 age. So the idea that this information can somehow get

16 out and get loose is not a fantasy.

17 This has, in fact, happened over and over again,

18 and sometimes the impact is worse on some populations

19 and not on others, and, therefore, I think the other

20 part of this assessment should include what Paul said,

21 that it depends on the population, and their particular

22 place in the ecosystem does make a difference in terms

23 of the effect of the harm and the impact of the harm.

24 And so perhaps that would inform whatever remedy was

25 offered by the government to the person who was harmed.

101

1 And then just sort of generally speaking, I fall,
 2 I think, in the category of -- the idea that -- of sort
 3 of Professor Calo's rubric on this, which is that there
 4 is subjective harm and objective harm, you know? So
 5 subjective harm is the perception of loss of control,
 6 and it's the sort of -- that results in kind of a fear
 7 or discomfort. And then, of course, there's the
 8 objective, which is where there's an actual adverse
 9 consequence. And, again, I think those should be
 10 divided by the idea of what is permissible, what raises
 11 risk, and what should involve consumer remedy.
 12 MR. COOPER: Thanks.
 13 So I think, you know, we're moving here from
 14 talking about -- we went down the first line saying what
 15 is harm, and if we're talking about an individual, we're
 16 talking about, you know, Carl, well, you know, again, as
 17 I mentioned, he may be harmed if people know about his
 18 greeting card habits, but when we're -- and, you know, I
 19 mean, legitimately.
 20 I mean, there could be -- I know it's hard to say
 21 that with a straight face, but by the same token, you
 22 know, everyone -- there is no accounting for taste, and
 23 everyone has their utility function, and economists are
 24 agnostic about that.
 25 MS. DE MOOY: Sure, and maybe he is buying it for

102

1 his mistress.
 2 MR. COOPER: Good. That will show up on next
 3 year's final.
 4 But when we think about regulation and
 5 government, we can't make -- at least not in this role
 6 yet -- we can't make individualized rules, right? So we
 7 have to look at distributions of -- we have to look at,
 8 you know, kind of the distribution, where we can draw
 9 the line.
 10 So I think that, you know, in this case, when we
 11 talk about the greeting cards, we think, well, we can --
 12 I think it would be pretty easy here to say that, well,
 13 there could be some people who are especially sensitive
 14 about their greeting card -- greeting card habits, but
 15 it would be -- it would be hard to see for me, you know,
 16 government intervention, especially some sort of
 17 aggregate or even individualized, like I want to have an
 18 algorithm to predict what kind of greeting cards people
 19 like and send out ads from my Hallmark store to say,
 20 well, try this greeting -- you seem to like these
 21 greeting cards, try this, because, again, you know,
 22 there may be some people way out on the tail, but we
 23 can't individualize our rules.
 24 But this -- and what I'll echo is something that
 25 both Paul and Michelle and I think Geoff -- maybe, maybe

103

1 not -- but, you know, I do think that the type of -- the
 2 type of data do inform that. So if we're talking now
 3 about the HIV status, I mean, for all the reasons that
 4 Paul and Michelle gave, I mean, there's a lot of --
 5 that's very, very sensitive -- that's very sensitive
 6 information, and I think here, when you think about
 7 what's the right enforcement posture, I mean, where
 8 would this -- where would we have government
 9 intervention, you know, I think you have to balance a
 10 lot of things.
 11 I mean, first, there's just a direct utility harm
 12 from Carl, okay? So some -- this data about my interest
 13 or actual purchase -- again, not clear yet -- but in HIV
 14 testing is out there. That's a legitimate loss.
 15 There's also dynamic losses, and I think this is maybe
 16 the flip side of what Geoff -- I like what, you know,
 17 Geoff had said, okay, this information -- this
 18 information is out there, and perhaps there -- perhaps
 19 there are benefits to that to Carl's partners, but you
 20 also have to think about incentives to acquire the
 21 information in the first place.
 22 So if I'm concerned about my HIV status being out
 23 there and it's something I want to keep private, well,
 24 maybe I will engage in privacy protective behaviors that
 25 keep me from learning that valuable information. So

104

1 there's kind of that dynamic part, and it's related to
 2 autonomy benefits from privacy. You know, how do you
 3 act under observation versus not observation? So, I
 4 mean, these dynamic things you have to consider.
 5 But, you know, there are also -- there are also
 6 beneficial -- the data being out there is -- as Geoff
 7 said, there's benefits to that. There are benefits
 8 potentially to the insurance company. So I think that
 9 it's a different balancing.
 10 I mean, we kind of look at where -- I think
 11 speaking as an economist, I mean, you want to unite
 12 information and control the person who's the highest
 13 valued user of that information, and maybe Carl's the
 14 highest valued user of his interest in HIV testing or
 15 his concern about that because of direct utility loss
 16 and because of the dynamic benefits that come from
 17 his -- you know, actually acquiring the information
 18 about his HIV status, which can be, you know, quite --
 19 quite beneficial.
 20 I would also agree here -- and I want to echo
 21 something Geoff said -- because I do think it's better
 22 to focus on uses rather than collection of data if we're
 23 thinking about a regulatory posture. You know, so I
 24 think that, you know, if we're concerned, say, about
 25 numbers eight and nine, like what the insurance company

1 is going to do with this data or what the boss does, I
 2 mean, you know, we -- you know, we could go all the way
 3 back to one and say we're just not going to allow you to
 4 collect any data in a drugstore at all, because
 5 drugstores are -- you are doing a lot of sensitive
 6 things in drugstores, so no retail tracking in
 7 drugstores. That could be one -- one because there
 8 could be this cascade of risk.
 9 But we could also just say -- if we're concerned
 10 about HIV status, we could say, well, look, you can't --
 11 you know, as an insurance company, you can't base
 12 insurance rates on HIV status, you know, if we're
 13 concerned about that outcome. We could say that
 14 bosses -- that employers are not allowed to fire based
 15 on HIV status if we were concerned about that.
 16 We do that in -- we, as a society, make cuts like
 17 that all the time, that there is certain information you
 18 can't act on. I mean, I think rather than suppressing,
 19 you know, truthful information, that it's better to just
 20 prevent the uses of that information where we can, and I
 21 think that, you know, that has -- that has the two
 22 benefits in that.
 23 So one is that if we suppress -- prevent
 24 wasteful -- like, if we don't want insurance companies
 25 to use this information, but we prohibit -- but we don't

1 bar them from using it, we just prohibit the collection
 2 of the data, well, nothing's going to prevent people
 3 from investing in signaling behavior.
 4 So if we're worried about this -- I mean, so you
 5 are going to get signaling, you are going to get people
 6 trying to come with -- hey, I don't have HIV. And the
 7 other thing is -- and we have seen this with some recent
 8 studies with the ban the box initiatives -- is people
 9 engage in statistical discrimination. So if there is
 10 something that is actually useful in making your
 11 decision and can't ferret -- you're not allowed to have
 12 that information, then they'll find proxies for that.
 13 And so there have been, you know, a couple of ban
 14 the box -- which is, you know, don't look at -- you
 15 can't -- there are about 25 states have them in
 16 different forms, but it basically says you can't look at
 17 whether you have a criminal record, at some -- you know,
 18 on a job application, and there's a good study by Agan
 19 and Starr, then another one by Doleac and Hansen, that
 20 basically -- basically finding the idea of ban the box
 21 is incredibly well meaning. You know, let's break the
 22 cycle of, you know, going to -- I go to prison, I get
 23 out, and there is no meaningful -- no one will hire me
 24 because I've been in prison, kind of this catch-22, so I
 25 just go back to criminal activity. So let's break the

1 cycle. Let's not allow -- and so we do this by
 2 suppressing truthful information.
 3 An employer may actually have a legitimate reason
 4 to say I don't want to do this. So what happens when
 5 you bar -- when you engage in ban the box? Again, the
 6 two really good studies that are out there, they show
 7 that, well, discrimination against African-Americans
 8 goes way up, I mean, like ten times lower call-back
 9 rates in New Jersey and New York after ban the box than
 10 before for African-American males between, like, 18 and
 11 25.
 12 So I say that by -- you know, their cost is
 13 suppressing truthful information. People want to make
 14 decisions based on info, but -- so the way to go is not
 15 to say you can't collect it. Just say you can't use it.
 16 So anyway...
 17 MS. MITHAL: Alessandro?
 18 MR. ACQUISTI: Well, I feel that, although coming
 19 from different directions, both Geoff and Paul made a
 20 point I agree with, which is not all injuries
 21 necessitate government intervention, and there may be
 22 countervailing benefits arising from those injuries.
 23 So the way I try to think about this problem, it
 24 is to go back, as I often do when I work in this area,
 25 to the seminal work on the economics of privacy coming

1 from Chicago School scholars in the seventies, such as
 2 Posner and Stigler. They pointed out that privacy
 3 protection is inherently really sticky, okay? It
 4 creates economic losers and economic winners. It
 5 affects the distribution of wealth.
 6 And I believe they were correct in pointing that
 7 out, but I believe also they stopped short of
 8 recognizing that also the absence of intervention, so
 9 the absence of protection, is creating winners and
 10 losers. There is no way out.
 11 If you intervene, you are going to affect the
 12 distribution of wealth. If you do not, you are still
 13 affecting by not intervening. So the dilemma for the
 14 regulator is how to choose whether to intervene or not.
 15 Some of my colleagues in the economics discipline
 16 believe that, well, when things are so complex,
 17 actually, take a step back. Regulate only when there is
 18 some dramatic, quantifiable, provable harm, and let the
 19 market do its magic.
 20 Well, as an economist, although I do believe in
 21 markets, I also have reasons not to believe that, in the
 22 case of privacy, they work that optimally. First, we
 23 have ample evidence, which we have described in the
 24 Journal of Economic Literature Review, we published last
 25 year, we have -- Curtis and Liad -- we have ample

1 evidence, theoretical and empirical, that without
 2 government intervention, it is not a given that the
 3 markets will end up with an optimal amount of
 4 information sharing, information protection, so from the
 5 aggregate perspective. So we already have that.
 6 Second, we also know that there are enormous
 7 information asymmetries when it comes to personal
 8 data -- how much information about myself is being
 9 collected, how it is being used, what the consequences
 10 will be -- which renders the individual responsibility
 11 argument, which is essential for good market outcomes,
 12 essentially untenable.
 13 So what do we do when we face a scenario where we
 14 have stakeholders' interests in contrast, in tension
 15 with each other, as it comes to how much data should be
 16 collected and analyzed? And these interests are not
 17 just economic interests; they also relate to things such
 18 as autonomy, freedom, and dignity.
 19 Well, I feel that the way to tackle this is not
 20 just to have a sound economic analysis, which we should
 21 have -- and this workshop is very useful in that
 22 direction -- but also listen to the will of the citizens
 23 through their elected representatives. That could be a
 24 good metric for government intervention. If a majority
 25 of others think that privacy is important, perhaps we

1 should listen to them.
 2 MS. MITHAL: Okay. So there's a lot to discuss,
 3 but I think we have to move on to the data security
 4 hypothetical, and we might get some time to come back to
 5 tie the two together, but -- so let me -- we will do the
 6 same exercise. We will read out a sentence from the
 7 hypothetical, and just raise your hand when you think
 8 that there is injury, okay? (Slide 22)
 9 So Company A stores consumer SSNs. A security
 10 researcher discovers that Company A has a security
 11 vulnerability that exposes its entire computer network,
 12 but no unauthorized access has occurred. (Acquisti and
 13 Ohm raise hands.)
 14 Okay. Two, unauthorized access occurred, but
 15 confirmation that no consumer data has been exfiltrated,
 16 okay? (De Mooy raises hand.)
 17 Unauthorized access has occurred, and it is
 18 possible that consumer data has been exfiltrated.
 19 Okay. Unauthorized access and consumer data from
 20 Company A has been found on the dark web, but there is
 21 no evidence that it has been used for a fraudulent
 22 purpose. (Cooper raises hand.)
 23 And then, finally, unauthorized access and
 24 consumer data from Company A has been used for
 25 fraudulent purposes. (Manne raises hand.)

1 Okay. So let's see, so why don't we -- we'll
 2 switch around the order this time with the -- why you
 3 raised your hands when you did. So why don't we start
 4 with James.
 5 And actually, we have about 34 minutes left. We
 6 have the data security hypo, hoping to wrap up, so if
 7 you could keep your interventions short, and we can
 8 probably get in a few more questions or issues to drill
 9 down.
 10 MR. COOPER: Okay. Yeah, so I went with number
 11 four just because at that point that's where I think
 12 that the risk of bad things happening is sufficient
 13 enough. I mean, you're on the dark web. We have
 14 evidence that these data are with bad actors for
 15 potentially bad purposes, essentially, and certainly
 16 number five, you're there.
 17 But one through three, at that point, it's too
 18 speculative to me to say. Again, it's a -- there's
 19 probably some increased risk of harm, but it isn't
 20 sufficient, and I don't know if at this point we're just
 21 talking about, you know, legal intervention or where we
 22 are in the hypo, but I would say one through three
 23 doesn't -- isn't sufficiently cognizable in my view.
 24 MS. MITHAL: Why don't we go this way -- oh,
 25 okay. Go ahead, Michelle.

1 MS. DE MOOY: Okay. So where I land on number
 2 two is a privacy violation, perhaps lesser on the
 3 assessment of harm, but still, nonetheless, a violation,
 4 and that is because -- I would go back to actually a
 5 former FTC Commissioner, Thomas Leary, who framed
 6 unfairness authority as "a tool best deployed in
 7 circumstances where third parties with whom consumers
 8 have no relationship do unfair conduct, practices prey
 9 on vulnerable consumers, involves coercive conduct, or
 10 creates significant information deficits."
 11 So my assumption on this -- and this could be
 12 incorrect -- but my assumption here is that the consumer
 13 is not aware of this unauthorized access and in this
 14 case I think should be made aware of it. So as we all
 15 know, the limits to what we understand versus the limits
 16 as to what hackers and others understand, there's a
 17 great information asymmetry there, too.
 18 In other words, if there was unauthorized access,
 19 I don't think that it's fair to assume that it's fine.
 20 In fact, I think it's fair to assume that it's probably
 21 out on some level. And so, you know, I think it just
 22 depends on which way you lean, which way you decide to
 23 assume, and I think, you know, from -- if you come from
 24 privacy as a core principle, you lean towards the
 25 protectionist idea.

1 And so, therefore, number two would not
2 necessarily trigger government intervention or laws but
3 that it might trigger some kind of awareness, some kind
4 of notice and control for the consumer to be made aware
5 of the unauthorized access and perhaps be able to take
6 their data away, out of the company who, in this moment,
7 has failed.

8 MS. MITHAL: Geoff?

9 MR. MANNE: I want to just -- let's see, I raised
10 my hand with the last one, and even it is actually
11 somewhat questionable, not that there's injury. There
12 obviously is sort of -- it's defined in terms of injury,
13 but in part to respond to what James said, I just wanted
14 to ask -- I hate to introduce my own hypothetical -- but
15 let me just ask, the Equifax breach, everyone agrees
16 that that was injury? Anyone not think that was injury?

17 So -- I don't know, no one raised their hands
18 either way. So no one thinks it's injury? The reason I
19 ask is because I -- you know, I don't know if this is
20 true or not, but I know that according to the IRS, of
21 the 150 million records that were exposed, some 100
22 million, they estimated, were already on the dark web,
23 that -- and the language they used in one place was we
24 actually think it won't make any significant or
25 noticeable difference.

1 Again, let's just take that as true for the
2 moment. It may very well not be, but I think -- so,
3 James, for example, pointed to number four. I think
4 that even number four -- and even, for that matter,
5 number five -- can't really be injuries so clearly.

6 Again, if the information was already out there
7 and if it was already being used for fraudulent
8 purposes -- now, there could be additional fraud and
9 there could be additional costs, so we can see how
10 number five could be an injury, but number four -- and
11 number four, too, it doesn't really matter if -- anyway,
12 it's whether the information is already out there, which
13 goes to this point about making risk of harm into a harm
14 itself.

15 I don't want to keep harping on this, but I will,
16 because I think it's really -- I think it's really
17 problematic here, especially in the data security
18 context where -- again, so we don't know anything about
19 any of the conduct here, all -- you know, we know that
20 unauthorized access occurred, for example.

21 Well, I can tell you that there is a nonzero
22 chance that even the most secure systems could be
23 subject to unauthorized access, and we know that because
24 the NSA was subject to unauthorized access, right? And
25 so -- and, again, in the narrow confines of this initial

1 question, that doesn't actually tell you anything about
2 whether there's been an injury or not, but I think
3 it's -- in other words, whether someone was harmed --
4 but I do think it's essential, when we're starting --
5 that the things -- as you've seen, as we've been talking
6 about this, they all blend together quite a bit, and
7 it's -- if we're going to be talking about risk, for
8 example, as being -- that risk of injury as being an
9 injury itself, I don't think we can talk about -- we can
10 talk about that without talking about the things that
11 create the risk.

12 And I find it especially problematic if we are
13 defining as injury something that can result from firms
14 taking the utmost, absolute, you know, blockbuster care,
15 well beyond what we would ever actually want them to pay
16 to take, and if that can still increase the risk of some
17 cognizable harm and, therefore, constitute injury,
18 again, I think we're -- things are really problematic
19 then.

20 So just to clarify, so maybe five, probably five,
21 but nowhere before five.

22 MS. MITHAL: Okay. So Paul, then Alessandro,
23 then James.

24 MR. OHM: So I warn the moderators, I am going to
25 fight the hypo, but I'll fight it very quickly, because

1 I know we are short on time, and then I'll answer it not
2 fighting the hypo.

3 Let me put another hat on. When I was a network
4 systems administrator before I went to law school, I
5 defended networks. If I ever met someone who said no
6 unauthorized access has occurred, we can confirm that no
7 consumer data has been exfiltrated, then you know that
8 serious violations have occurred, because those are
9 naive statements. Those are impossibilities, right? We
10 can never be sure of things like that.

11 And it's the companies that are sure that their
12 data has not been exfiltrated because their Sys Admin
13 said we have an IDS, those are companies that I
14 guarantee you are like, you know, just crawling with
15 hackers at the time. So fighting the hypothetical, I
16 want the government to investigate number one because
17 that company is naive or lying, okay, but let me not
18 fight the hypothetical, right?

19 So another way to kind of respond to Geoff's
20 comments is do we find a world in which Equifax has
21 occurred to be an acceptable state of the world, right?
22 Is this a problem that we, as a collective and as
23 individuals, should try and solve? And I think that is
24 tied to the injury question, right?

25 Before Equifax, there was another -- you know,

1 there was a company a week who would demonstrate to us
2 time and time again that, to speak like an economist,
3 there are externalities that need to be internalized and
4 they are not, under whatever mechanisms we have. The
5 state of data security in the world is horrid, is
6 horrible, and is causing concrete repercussions for
7 everybody in this room.

8 I, like Elizabeth Warren -- I like saying I like
9 Elizabeth Warren -- spent three hours on the phone and
10 on the website trying to, like, go through the Byzantine
11 data monitoring protocols that they have, and I wasn't
12 able to do that after three hours. That's time wasted.
13 There has been anxiety, people face financial ruin,
14 right, people self-chill, they self -- they change their
15 behavior.

16 They don't apply for jobs they might apply before
17 because they are worried about their credit report.
18 They don't try and buy a house because they know they
19 are not going to get a home loan. And there are
20 documented cases time and time again -- and Geoff has
21 impressed upon us several times -- that we should look
22 for documented cases. They are not hard to find.

23 And so for all of those reasons, I think all five
24 of those can be defined as injury, particularly if we're
25 not asking, is it actionable and legally redressable.

1 But let me end these comments with one point of
2 agreement with Geoff, which is, yeah, I absolutely agree
3 that we should account for how reasonable your data
4 security was, right?

5 If the world's greatest hacker broke into the
6 world's greatest security, then yes, the law probably
7 should not offer redress against the world's greatest
8 security purveyors, because they're behaving
9 responsibly, and they have internalized the externality
10 that I'm talking about.

11 It doesn't make it less harmful, but it does mean
12 that there might be some notion of causation or
13 countervailing benefit or something else that we should
14 take into account. And so, yes, I think I agree with
15 you there that, that in making these hard choices, we
16 should think about how good was your security at the
17 time.

18 MR. ACQUISTI: I raised my hand for number one
19 for reasons similar to the ones Paul mentioned and very
20 similar to the ones I brought out under the previous
21 scenario, where there are boundaries, and whether the
22 consumer even knew that the company, Company A, stores
23 his or her SSN, whether Company A had a right to, in
24 fact, have this information, how did it acquire this
25 information, why and how it is using this, et cetera, et

1 cetera, et cetera.

2 Now, again, I will agree that not necessarily
3 quantifiable, realizable economic damage had occurred,
4 but the possibility of it -- in fact, there's increased
5 risk of the downstream cost, which allows me to go back
6 to a promise I made earlier in the more technical
7 discussion of the economic harm, right?

8 Even if you want to narrow down the definition of
9 injury to economic harm, then we have to face the
10 enormous challenges of quantifying the term even when we
11 know that it does exist. The challenges are enormous,
12 and I will give you some examples.

13 One is that the harm is incredibly context-
14 dependent. The very same piece of information could be
15 harmless or even beneficial in one context and extremely
16 damaging in another context. The harm can take very
17 different economic typologies. There is the direct
18 harm, such as Carl being fired or this consumer data
19 being used for fraudulent purposes.

20 There is the opportunity cost. If my data is
21 used by others, my ability to use it strategically
22 decreases. There is the loss of earning. Someone else
23 may be benefiting from my data, and perhaps I'm not
24 getting a fair share from that -- those benefits.

25 And then there are also other differences, other

1 nuances, which, again, make it incredibly hard to
2 pinpoint, quantify the harm. There are costs which are
3 exceedingly small but happen continuously. The time I
4 have to spend deleting the Spam message which my Spammer
5 filter didn't catch, the increasing time, perhaps few
6 fractions of a second, but across many consumers and
7 across a long period of time amount to a huge waste of
8 time due to the fact that when I log a page on the
9 internet, the page is loading in its loader because of
10 the tracking going on behind the browser.

11 On the other hand, on the opposite end, there are
12 the costs which are catastrophic but are very low
13 likelihood, such as catastrophic medical identity theft.
14 And then the differences between the harms which occur
15 immediately after some privacy invasion has occurred,
16 and in your example, scenario one, Carl's employer
17 firing Carl immediately after this information has
18 arisen, and the harm which may take -- which may happen
19 months or years after the fact, such as maybe someone
20 suffering from the Equifax breach one year from now,
21 making it incredibly hard for us, as economists, to
22 prove causality, even though there is a high suspicion
23 that there is a direct link.

24 So the point being that these costs are so
25 diverse and so nuanced, the idea that we can create just

121

1 a simple metric to capture them all and their -- and a
 2 simple formula that the regulators can use to decide,
 3 oh, yes, I should intervene, or no, I shouldn't
 4 intervene, is really hard, seems almost to have a
 5 premise that is untenable to me.
 6 MR. CHILSON: Well, great. Thanks to all the
 7 panelists for walking through the hypothetical and
 8 identifying why you raised your hand at the point, even
 9 if you didn't all embrace the hypothetical as written.
 10 But, James, you wanted to respond?
 11 MR. COOPER: Yeah. Well, I just wanted -- I
 12 guess since I put my tent up, a lot has been said.
 13 First, I am going to agree with both Paul and
 14 Alessandro. I mean, this is, as an economist -- I mean,
 15 there are -- as far as internalizing the externality, I
 16 mean, it's hard to think of how this can happen, but for
 17 all the link between, you know, I committed -- you think
 18 of the normal tort. I drove carelessly, I hit somebody,
 19 they got hurt, and that's easy, causation, you know, and
 20 then you -- so you said you calibrate toward law to
 21 internalize that. That can't be done here.
 22 I mean, it is really -- as far as linking, I
 23 think it's very difficult, and I think that one thing we
 24 have to think about as we go forward and think about how
 25 to deal with -- and I think this tees off of -- goes off

122

1 on something Michelle had said and a theme throughout,
 2 is, you know, there's data everywhere. There's -- we
 3 don't know, if there's a breach, where that data came
 4 from.
 5 Ultimately, as a system, I mean, we think -- if
 6 this is something we just live with, I mean, do we think
 7 of this as a first-party insurance world, where we just
 8 kind of all either self-insure or buy insurance policies
 9 against cyber risk and just let -- and then we reduce
 10 some of the -- some of the incentives that tort can
 11 potentially bring, but it's hard -- for the reasons that
 12 Paul actually talked about in the previous case, you
 13 know, that many or if not most data breach cases get
 14 thrown out either for lack of standing or lack of
 15 meeting -- pleading harm sufficiently. So, you know,
 16 the tort system, it's unclear.
 17 So, you know, it would -- does it make sense to
 18 have first-party -- you know, to -- rather than being
 19 insured through the court system, to add first-party
 20 insurance, and then maybe backed up by some kind of FTC
 21 intervention when applicable? I'm not sure.
 22 I do think it's super-complicated, but when I
 23 first put my tent up, I did want to kind of amplify
 24 something that Geoff had talked about is risk, and I do
 25 think that this is the big question. You know, as Geoff

123

1 said, maybe -- you know, I raised my hand at number
 2 four, but, you know, you raise a valid point, that,
 3 okay, number four, even number five, so there's harm. I
 4 mean, you were kind of fighting the hypo --
 5 MR. CHILSON: If it was unclear, next year we
 6 will write the questions more clearly.
 7 MR. COOPER: Yeah, yeah, well, that's how I --
 8 but the idea that we can't -- it is going to be really
 9 hard to link up. So it's on the dark web. Maybe it was
 10 already on the dark web, and maybe it's on the dark web
 11 that has nothing to do with this data breach, you know,
 12 and so I think about this, and, you know, I was -- like
 13 probably everyone in this audience, I think about this
 14 as like a Bayesian updating problem -- that's a joke, by
 15 the way, or maybe it's not, maybe it's not, maybe
 16 everyone is thinking exactly like that -- but I think
 17 you kind of start off with some kind of view -- you
 18 know, prior view of the world for the odds of my data
 19 being misused as part of a breach, and then, you know,
 20 ultimately what we're trying to figure out is what are
 21 the odds that this breach is going to lead to some kind
 22 of demonstrable -- this conduct, whatever -- not the
 23 breach, I'm sorry, the conduct -- the vulnerability that
 24 this firm is engaged in, likely to lead to harm.
 25 And so what you think about, you update your

124

1 priors by thinking how often, when I see a breach, is it
 2 associated with this kind of conduct? I mean, that's
 3 what's called a likelihood ratio in updating, and so the
 4 thing is, is how much does what we know change our --
 5 about the -- the likelihood that this conduct is related
 6 to harm change our -- change our priors? And it could
 7 be that this really -- the delta, the change in the odds
 8 of harm are really, really high. It could be like a
 9 factor of two, but it also could be that the baseline of
 10 harm conditional on breach is so small that the
 11 posterior, my final -- you know, so it moves from the
 12 odds of harm from this breach being 1 percent to 3
 13 percent.
 14 So at that point, do we look at the delta, which
 15 could be really large -- and these are like
 16 epidemiological studies, where you start with a really
 17 low baseline of a -- some kind of condition, and then
 18 there's a drug, and the drug reduces that condition by
 19 four times, but it just goes from like, you know, 3
 20 percent to 2.5 percent overall. So it's the same kind
 21 of thing. Do we look at the change in the risk or do we
 22 look at the overall risk?
 23 And I think that -- to me, I don't know exactly
 24 where I come out on that. I know that there's a case
 25 whose name can't be spoken up here that that's one

1 theory, is to look more at the delta in harm, look at
 2 how this conduct is likely to change the likelihood of
 3 harm as opposed to the overall incident of it.
 4 And also, I know that this is -- we haven't
 5 really gotten into this, but, you know, the extent to
 6 which we actually -- the conduct has been out there and
 7 it hasn't happened for a while, I think that does
 8 inform, but -- but anyway, I see other people with their
 9 tents up, so I will not go on.
 10 MS. MITHAL: Geoff?
 11 MR. MANNE: I will be much quicker than James
 12 was. In fact, I was going to put what James said into
 13 English.
 14 MS. MITHAL: Thank you.
 15 MR. MANNE: I think there's a big problem --
 16 MS. MITHAL: Epidemiological?
 17 MR. MANNE: -- in -- no, actually.
 18 No, I think that there's a big problem, and it
 19 was reflected in what Alessandro said and what Paul
 20 said. No question this is really complicated, and James
 21 makes great points about assessing risk as a -- I won't
 22 repeat everything he said, but all of that and all of
 23 that discussion and all of the discussion, the
 24 acknowledgment that there are problems out there and
 25 that certain conduct actually can cause harm or cause a

1 risk of harm, I mean, all of that says nothing about the
 2 optimal level of injury, the optimal level of data
 3 security breaches, and the optimal level of care that's
 4 supposed to be taken.
 5 And I sympathize or I agree, in fact, with
 6 everything everyone has said on this score, except
 7 nothing they've said is really operationalizable or even
 8 really particularly relevant until they've established
 9 that we're deviating from the -- from optimal or from
 10 some identifiable baseline, because while we can point
 11 to lots of injury, as long as we're all going to
 12 acknowledge that the cost of making the injuries zero or
 13 the risk of injury zero is far higher than we are
 14 willing to pay, you haven't yet established that we are
 15 actually at a point where we should be intervening more
 16 or identifying more, looking at changes in risk, you
 17 know, from 1 percent to 3 percent as actionable, and all
 18 of those things are totally possible, except none of
 19 them can be determined unless we have some better sense
 20 of what the optimal baseline is, and I don't think we
 21 have anywhere close to that. Thank you.
 22 MS. DE MOOY: Okay. So I reject that, and I will
 23 get to that in a second, just a second.
 24 MR. MANNE: It's tautological.
 25 MS. DE MOOY: One thing that I want to say, just

1 to push back on something, James, that you said about
 2 tort, which is that the tort of assault requires
 3 imminence, and I think you were saying that wasn't part
 4 of that assessment when it is.
 5 MR. COOPER: No, the imminence is -- like the
 6 tort has -- it has been -- these cases have been thrown
 7 out, most of them have been thrown out either on
 8 standing grounds, or even if they make it past standing,
 9 they -- so I think we were in agreement.
 10 MS. DE MOOY: So I just want to finish my
 11 thoughts. So I think -- you know, fine, but I think the
 12 point that I want to make is that the FTC can look at
 13 these issues in a much broader, richer way than the
 14 court system, right? I mean, we can look at social
 15 harms in a way that the court system cannot. I think
 16 that's an important part of determining how to govern
 17 here.
 18 And so I think that the imminence of -- is akin
 19 to the idea of risk, and I think that's important. I
 20 think -- I just want to also mention, while we still
 21 have time, that I think the way that the FTC can
 22 approach this to respond to your sort of fatalistic
 23 feeling that we can't actually --
 24 MR. MANNE: No, optimistic. I'm saying we have
 25 to do it, that we should do it.

1 MS. DE MOOY: We do have to do it, and I do think
 2 that there are, baselines, like no breach. There's a
 3 baseline. Now, the idea of how you penalize breach or
 4 practices, of course, is up for grabs, and I think there
 5 are ways to do that also. There are precedents for what
 6 is permissible in data security, and, of course, those
 7 might change over time. And so this has to be a fluid
 8 framework that can do that.
 9 I think unfairness has that potential. I think
 10 unfairness has a much broader reach than deception, and
 11 I think that is where the FTC can begin to explore how
 12 to assess a risk, how to assess harm in that framework.
 13 For example, you have -- you know, it -- under the FTC
 14 Act, substantial injury cannot be reasonably avoidable,
 15 is not offset by benefits, right?
 16 So all of the sort of areas that I mentioned, the
 17 idea that it can't be readily avoidable is a huge issue.
 18 This is absolutely impossible most of the time for
 19 people to avoid being in this database in the first
 20 place. It is not necessarily possible. Many, many
 21 people I spoke to had no idea that Equifax existed or
 22 had data on them, right?
 23 So, I mean, the information asymmetries, the lack
 24 of a level playing field I think is absolutely crucial,
 25 and you cannot just sort of go past that and say that

1 that's not a part of the risk assessment. It has to be
 2 a huge part of the risk assessment, and I think the way
 3 to do that for the FTC is through the unfairness
 4 doctrine.
 5 MR. CHILSON: Great. Do you guys want to put
 6 your cards down?
 7 MS. DE MOOY: Oh, sorry.
 8 MR. CHILSON: I don't want to keep calling on
 9 you.
 10 MR. MANNE: I have more to say.
 11 MR. CHILSON: So one thing that I -- tying
 12 together the responses to the two sets of the
 13 hypotheticals, while Paul openly admitted that he was
 14 pushing back against the hypothetical, I think pretty
 15 much all of you pushed back, which is the point of
 16 hypotheticals, and I was particularly interested in,
 17 both Michelle and Alessandro, you both said -- not in
 18 exactly the same terms but essentially -- like, this
 19 might not be harm -- and I think, Michelle, you actually
 20 did say this -- might not be harm, but it is a
 21 violation.
 22 And so I am interested in teasing out why the
 23 difference there, and I think, Alessandro, you sort of
 24 laid out a sort of -- a boundary framework, that when
 25 you cross the boundary, that's a type of harm, and I

1 think it sounded to me a little bit like, Paul, you
 2 pushed back against that idea a little bit in the sense
 3 that injury is a sort of collective thing that we've
 4 developed over time and that law has a role to play in
 5 that.
 6 So I just wanted to throw that out there for the
 7 panel, whoever is interested in talking about that, but
 8 especially Alessandro and Michelle, about why would we
 9 have violations where there aren't harms?
 10 MR. ACQUISTI: Well, my two points on this would
 11 be that there are violations which may not arise to
 12 economic harm, but other forms of harm, autonomy or
 13 dignity or freedom.
 14 Secondly, there is the increased likelihood of
 15 downstream harm, and then we can debate, as we did on
 16 this panel, whether the increased risk we felt
 17 materialized damage is enough for intervention or not.
 18 That's a fair point to debate.
 19 And third, there are all these categories of
 20 economic harm which we know are there, but we find it
 21 very hard to quantify. So this is in a sense my
 22 argument.
 23 And the last point I will make, if there is -- if
 24 there are a few more seconds, is that I would suggest
 25 that as important as this workshop and type of panel is,

1 I would suggest also a different workshop, a different
 2 type of panel, where the burden of proof is not put on a
 3 consumer, demonstrate that you have economic damage,
 4 otherwise, we should not -- we should not intervene to
 5 protect, but the burden is twisted around and put the
 6 data holders into the position of demonstrate that you
 7 cannot do these transactions you are doing now in a more
 8 privacy-protective manner. And if you do, and if you
 9 claim that there are costs of doing so, demonstrate --
 10 tell us, show us -- where the costs go. Only to you?
 11 To consumers? To society?
 12 So for the moment I am going back to the
 13 essential problem we are facing here, which is enormous
 14 information asymmetry at the individual level, because
 15 individuals don't know how information about them is
 16 being collected or used, and then societal level,
 17 because as much as we like to believe in data analytics,
 18 much of the internal data economy right now is a black
 19 box where we do not exactly know what is happening. We
 20 know that value is being generated. We don't know
 21 exactly how it is being allocated. That is to me a
 22 pretty crucial question that, as economists, we should
 23 address.
 24 MR. CHILSON: Great.
 25 Michelle?

1 MS. DE MOOY: I think that was well said. I
 2 think the only thing I would add is that the person --
 3 you know, privacy is contextual, as we know, and,
 4 therefore, an individual's perception of the situation
 5 matters, and I think the way that the government can
 6 play a role there in leveling the playing field here is
 7 by assessing what are reasonable expectations, what
 8 types of user controls are available to this person,
 9 what sort of access rights do they have.
 10 And then when we move down the spectrum of risk
 11 to economic or quantifiable harm, that's when you can
 12 assess whether remedy makes sense, whether there is a
 13 justifiable remedy. And I think that is logical and
 14 exists in so many of our laws, but for some reason, as
 15 Alessandro kind of pointed out, this is skewed in this
 16 environment as if the benefits of data collection are so
 17 great to consumers that it's ridiculous to think that
 18 there could be sort of violations to harm, but I think
 19 that's absolutely what occurs and I think has been borne
 20 out, you know, in example after example.
 21 MR. CHILSON: Paul, we have some questions from
 22 the audience, so --
 23 MR. OHM: All right, go ahead. I'll find a way
 24 to say my answer in response to whatever you ask me.
 25 MR. CHILSON: Great. I trust that that is true.

1 So we have a couple questions here. Some of them
 2 have been somewhat addressed since I got them, so I am
 3 going to focus on one that has not been addressed yet,
 4 and I am open to you guys taking it in any direction,
 5 but a focus on harm would be particularly interesting.
 6 The question asks -- considering the panel -- do
 7 you all accept the notion that privacy is a critical
 8 component of democracy, as Michelle stated? Kind of a
 9 big picture question, but if you can tie it back to
 10 harm --
 11 MR. OHM: I totally have a segue to the point I
 12 was going to make.
 13 MR. CHILSON: Let's start with Paul, then.
 14 MR. OHM: Yes. So let me start small and I will
 15 end up at the question. So I wanted to respond to the
 16 Bayesian brothers, the idea that we are going to examine
 17 the delta --
 18 MR. COOPER: I didn't know I had a brother.
 19 MR. OHM: Yes. So what I find problematic about
 20 using that as the sole way of defining harm in a data
 21 breach case is it means if you are in a space where
 22 there really isn't much harm and there is a lot of
 23 responsible practice and then there is one really bad
 24 actor who is below the standard of care, then the FTC
 25 has jurisdiction, but then as the world goes to hell in

1 a handbasket and we end up in a cesspool, where all
 2 corporate actors, for whatever reason, you know,
 3 malevolent or benign, are not protecting us, are causing
 4 anxiety, causing the kind of fear I'm talking about,
 5 then suddenly you've stripped the agency of
 6 jurisdiction, that seems completely backwards and a
 7 little warped to me.
 8 It feeds to a point that Alessandro has made a
 9 couple times, but I think because he's an economist and
 10 because he's a polite Italian, he hasn't made quite
 11 forcefully enough, which then leads to your question,
 12 which is -- Alessandro has repeatedly said that the
 13 economic tool kit can be very helpful when it talks
 14 about harm, but it should not be considered complete,
 15 right?
 16 And don't mishear me, we still should be
 17 empirical and we still should be rigorous, but I think
 18 in many ways the economic tool kit is deficient when it
 19 comes to this. And I know I'm talking to an agency that
 20 happens to have a Bureau of Economics, that has people
 21 who helped put this workshop together. I think we need
 22 to look at other social sciences, we need to look at
 23 legal scholarship, and we have to understand, as you get
 24 into the very next panel, that sometimes it's going to
 25 be hard to kind of measure results that come from those

1 other fields with what the economists say. And if
 2 you're only looking to the economists, you're thinking
 3 of this too narrowly, which goes to democracy, right?
 4 So the idea here is there are absolutely ways --
 5 whether or not democracy falls within the FTC's core
 6 mission, I don't know if I'm ready to say it -- but
 7 there are ways of saying that when we talk about privacy
 8 harm, we are talking about broader societal problems,
 9 and Congress in its infinite wisdom said, look, the
 10 courthouse doors are going to be open or not to
 11 traditional tort law principles, but we are going to
 12 write a capacious, broad statute because we can't read
 13 the future, and we want to create an agency that can
 14 stand by the consumer today and tomorrow and the day
 15 after, and I think that's how they wrote their
 16 unfairness provision, and I think it's kind -- a
 17 responsible agency would take advantage of that and try
 18 and protect consumers in the way that Congress had in
 19 mind.
 20 So thanks.
 21 MR. CHILSON: Yes.
 22 Geoff?
 23 MR. MANNE: Well, I think absolutely it's the
 24 case that privacy from the government is essential to
 25 democracy. I think we have to always bear in mind that

1 we're talking about private entities here and our fellow
 2 citizens, and I think it's -- I think often -- not
 3 always, certainly, but often the two are allied and then
 4 they are extremely, extremely different in my mind. And
 5 we do a real disservice when we say something like, you
 6 know, the drugstore in the first example knowing
 7 something about me is -- not that anyone said this, but
 8 one could say -- is the -- you know, it's just as bad as
 9 the government knowing this about me, right? The next
 10 hypothetical after the insurer and the employer could
 11 be, you know, the government. And I think it's crucial
 12 that we keep those things separate.
 13 With respect to the ability to keep information
 14 private as being - sort of from other people as being
 15 crucial to democracy, I don't even really know where to
 16 begin to answer that, and that -- and therein lies the
 17 problem with what Paul just said. No one knows where to
 18 begin to answer that, and Paul is right, that one could
 19 read an immense amount of discretion into Section 5, and
 20 we could have an FTC that supercedes every legislature
 21 in the country and every other statute in the country,
 22 and indeed, you know, you could say that's what Congress
 23 intended. I mean, you'd be wrong, but you could say it.
 24 And the idea that sort of trying to implement
 25 some idiosyncratic principle like democracy at the level

1 of enforcement against real companies engaging in real
2 commerce with real consumers who are, for the vast,
3 vast, vast, most part of the time enormously benefited
4 by that -- something else to remember when we talk about
5 all this, we highlight all of the problems -- but as a
6 practical matter, to me, they are kind of few and far
7 between, really.

8 That doesn't mean we shouldn't care about them,
9 doesn't mean we shouldn't do something about them, but
10 let's not forget that they are the exception, not the
11 rule, and -- anyway, in sort of authorizing an agency to
12 say, well, we're protecting democracy, and, therefore,
13 we should be able to do basically anything we want,
14 without having a need or an ability to quantify it
15 strikes me as so dangerous as to undermine democracy.

16 MR. CHILSON: James?

17 MR. COOPER: All right. Thank you, Geoff, for
18 going on long enough that I might get the last word.

19 MS. DE MOOY: I will just reaffirm what I said
20 before and say that I don't think that anyone was
21 suggesting what you just said --

22 MR. CHILSON: Sorry, James raised his card.
23 That's the only reason I moved past --

24 MS. DE MOOY: Oh, I see. Okay.

25 MR. COOPER: No, no, go ahead, and then I will

1 say the last thing.

2 MS. DE MOOY: You get the last word. I would
3 just say, yeah, I don't think anyone was suggesting this
4 lawless world of, you know, immeasurably damaging our
5 democracy through the FTC's unfettered -- you know, I
6 don't think anyone was saying that at all. In fact, I
7 think the point of the FTC's involvement in privacy
8 is -- first of all, it's an agency of the United States
9 Government which is charged with protecting the
10 Constitution, which, of course, is embodied by
11 democratic values, and some of those include the space
12 for political thought, the space for choice, the space
13 for control, the space for deciding who can see
14 information and who cannot.

15 All of -- a lot of the data ecosystem violates
16 these principles in different ways, and so, therefore,
17 we can look at -- deeply into those to figure out what
18 exactly what makes sense for the FTC's role here. And,
19 again, I think it has a lot to do with leveling the
20 playing field, and that is a democratic principle, to
21 not have information asymmetries dictate all of these
22 practices and policies, but to have the level playing
23 field where the American consumer can make a choice.

24 And just incidentally, I would also say that the
25 distinction between government and commercial entities

1 is much blurrier than I think you were painting it to
2 be. You know, the government is acquiring commercial
3 data all the time. They are working with private
4 contractors all the time. So I think, you know, the --
5 it's not possible to make that distinction, per se. I
6 mean, in law we can, maybe, but in this discussion, I
7 think, you know, especially when you talk about health
8 data, which is more my area of expertise, it is
9 absolutely -- the government is constantly selling and
10 buying commercially generated information about people.

11 MR. CHILSON: James. Two seconds, James.

12 MR. COOPER: Yeah, okay, and Paul's wrong. No,
13 I'm just kidding.

14 The only thing I would say directly to Paul is
15 you had said that we -- the FTC needs to think -- you
16 know, incorporate a lot of other things other than the
17 economics. I think actually that's one of the issues,
18 is you say legal scholarship needs to be incorporated.
19 I think there has been very little, if any, economic
20 incorporation into a lot of the privacy, if you look at
21 the two privacy reports. So I think that moving away
22 from the legal scholarship, more into empirical work, or
23 at least balancing them more, I think that would be -- I
24 think the balance is certainly more on the other side.

25 But the last thing I'll say, I agree with, you

1 know, the question about democracy. I would agree with
2 Geoff, I think, when it comes to privacy. It's
3 vis-à-vis the government, not really vis-à-vis private
4 corporations, and I think the big -- you know, I'll
5 leave it at this. I think one of the big picture
6 questions here is, you know, I completely agree with
7 the -- that there are information asymmetries here, and
8 there are -- Alessandro's great body of work has shown,
9 you know, a lot of, you know, this contextual
10 dependence, a lot of biases and Dahlman effect exist in
11 this, but there -- asymmetric information and behavioral
12 biases exist across a lot of markets.

13 The question -- I think the big picture question
14 here -- and I will just end on this -- is, you know, we
15 think about what we want to do. What's better at
16 mediating consumer preferences in this case, the market
17 or the government? And I think that that -- the more
18 it's informed with empirical literature, I think the
19 better. So I will just leave it at that.

20 MR. CHILSON: Yep. Well, thank you very much to
21 our panelists, and thanks to all of you. I believe up
22 next we have lunch.

23 (Applause.)

24 (Whereupon, at 12:46 p.m., a lunch recess was
25 taken.)

1 AFTERNOON SESSION
 2 (1:46 p.m.)
 3 PANEL 3: BUSINESS AND CONSUMER PERSPECTIVES
 4 MS. HAN: All right, if folks could take their
 5 seats, we will get started with this afternoon.
 6 Okay, everyone, welcome back. Dan and I will be
 7 moderating this next panel, which will build on this
 8 morning's discussion and explore how businesses and
 9 consumers perceive and evaluate the benefits, costs, and
 10 risks of collecting and sharing information in light of
 11 potential injury.
 12 The panel will examine the considerations
 13 businesses take into account when choosing privacy and
 14 data security practices and also how consumers make
 15 decisions about sharing their information. So we are
 16 lucky to have a great group of panelists here with us
 17 for this discussion, and we will take questions at the
 18 end. So just as a reminder, there are comment cards
 19 available in the hallway and also with FTC staff inside
 20 the auditorium. If you just fill it out, raise your
 21 hand, someone will come and get it from you. For those
 22 of you viewing the webcast, you can submit questions via
 23 Twitter.
 24 Now I would like to introduce our panelists. So
 25 closest to me is Omri Ben-Shahar, who is the Leo and

1 Eileen Herzel Professor of Law and Kearny Director of
 2 the Coase-Sander Institute for Law and Economics at the
 3 University of Chicago Law School. He teaches contracts,
 4 sales, trademark law, insurance law, consumer law,
 5 e-commerce, food law, law and economics, and game theory
 6 in the law, and writes primarily in the fields of
 7 contract law and consumer protection.
 8 Next to Omri is Leigh Freund. Leigh is the
 9 president and CEO of the Network Advertising Initiative,
 10 where she leads the organization's growth and helps with
 11 the agenda and strategic priorities. Leigh joined NAI
 12 in 2015, after an 11-year career at AOL, where she
 13 served as vice president and chief counsel for global
 14 public policy.
 15 Next we have Jennifer Glasgow, who has served as
 16 a global privacy and policy executive for over 40 years,
 17 originally with Acxiom and most recently with First
 18 Orion Corp. She is very active in numerous
 19 international efforts to develop effective public policy
 20 with maximum harmonization across the world.
 21 Then we have Bob Gourley. Bob is cofounder and
 22 partner of the cybersecurity consultancy Cognito, which
 23 helps companies fight cyber crime and corporate
 24 espionage. He is the author of the book The Cyber
 25 Threat. His first career was as a naval intelligence

1 officer, and he was the first director of intelligence
 2 at the Department of Defense's Cyber Defense
 3 Organization.
 4 And last, but not least, we have Katie McInnis.
 5 Katie is a policy counsel in Consumers Union's
 6 Washington, D.C., office. Her work focuses on
 7 technology and the consumer's right to privacy,
 8 security, control, and transparency. Before joining
 9 Consumers Union in 2016, Katie served as a privacy and
 10 technology fellow at the Center for Democracy &
 11 Technology, and in the Enforcement Bureau of the Federal
 12 Communications Commission.
 13 So thank you again to our panelists for joining
 14 us today.
 15 MR. WOOD: Okay. So the format of this panel is
 16 basically going to be a loosely organized group
 17 discussion, and we are going to start off with some
 18 business-oriented questions. The first one is pretty
 19 broad.
 20 So what are the risks and benefits businesses
 21 consider when deciding whether and how to collect and
 22 share consumer information?
 23 MS. FREUND: Good afternoon, everybody. Thanks
 24 for having us on the panel this afternoon. We are
 25 thrilled to be here. I represent the digital

1 advertising industry here, and we represent third
 2 parties, first parties, and other companies involved in
 3 the digital advertising ecosystem. So when we think
 4 about the benefits and the risks and how companies are
 5 weighing the benefits and risks of the use of data
 6 that's collected online, you know, we think through kind
 7 of the entire internet ecosphere.
 8 So, you know, revenues from online advertising
 9 support the free internet. I know that's a very broad
 10 statement, but we support and facilitate e-commerce. We
 11 subsidize the cost of content and services that
 12 consumers really value and expect, and this is a really,
 13 really valuable kind of benefit.
 14 We have to weigh that with the risk of what are
 15 we doing with consumer data and what are consumer
 16 expectations, which is something I think we will get
 17 into in a little bit, but, you know, we have got just
 18 some statistics to share with you.
 19 Eighty-five percent of consumers in a survey that
 20 was conducted by the DAA, which is one of our fellow
 21 trade associations, say that they prefer kind of an
 22 ad-supporting internet model so that they don't have to
 23 worry about paying for costs and services, and so, you
 24 know, online marketing has really big, direct,
 25 significant benefits for consumers. It helps them

1 connect, create, publish.
 2 You know, we are talking not just about Google
 3 and Facebook when we talk about the internet, but we're
 4 talking about my favorite hypothetical example,
 5 joesknitting.com. We can support advertising that
 6 supports joesknitting.com to be able to reach their
 7 consumers because the advertisements are reaching
 8 individual users as they travel across the internet and
 9 not individual websites. And so we support kind of the
 10 long tail of publishing online and contents and services
 11 that consumers might not otherwise be able to access.
 12 So when we think about risks, however, part of
 13 our genre is self-regulation in this internet
 14 advertising ecosystem, and so we think about what are
 15 the specific, concrete injuries that cause or are likely
 16 to cause kind of substantial injury or harm to
 17 consumers. You know, we think through the Section 5
 18 framework about how things are not reasonably avoided by
 19 consumers and what are the benefits to consumers.
 20 So we think through data practices that are
 21 reasonable. We try to think about the types of injuries
 22 that might be quantifiable and economically harm a
 23 person. We think through some things like eligibility
 24 for employment. We think about eligibility for
 25 insurance requirements, and now we collect and use a lot

1 of data in advertising, and the serving of a targeted ad
 2 to you or to me because of our interests online is
 3 different and so weighed differently than the actual use
 4 of that data to make a decision around eligibility for
 5 employment or other things.
 6 And so we've got guardrails set up in our own
 7 environment, in our self-regulatory code, that kind of
 8 thinks through these potential concrete injuries and
 9 puts restrictions on our company's use of that data. So
 10 when we think about benefits and risks, we really try to
 11 spend some time thinking specifically about how to avoid
 12 the risks that might be inherent.
 13 We heard about some of them already earlier, in
 14 the earlier panels, and we try to put guardrails around
 15 them so that we can have responsible but vibrant data
 16 collection and use throughout the internet.
 17 MR. WOOD: Great.
 18 So, actually, when you -- to make things easier,
 19 let's raise our name cards when we -- if you want to say
 20 stuff.
 21 Jennifer, please go ahead if you were going to.
 22 Sorry.
 23 MS. GLASGOW: You want me to answer the same
 24 question, right?
 25 MR. WOOD: Sure. Yes, yes.

1 MS. GLASGOW: Okay. Well, my experience is in
 2 both marketing, so I'm very familiar with what Leigh and
 3 NAI have done, but also in risk management and
 4 government use of data. So I feel like, you know, when
 5 businesses are trying to assess the risks of information
 6 collecting and sharing, they tend to start by saying
 7 what are the benefits, what are the opportunities that
 8 information creates?
 9 And the reality is -- and you probably got a
 10 sense of this from the morning panels for those of you
 11 who were here -- the reality is that every piece of
 12 information that you collect has the potential for some
 13 benefit, and it may be different. It may be many, many
 14 benefits. Very rarely does a piece of data stand alone
 15 and only create value in one instance.
 16 However, there's two sides to that or that sword
 17 is sharpened on both edges, because there are risks, as
 18 Leigh has mentioned, that need to be taken into
 19 consideration. We look at laws first to decide, you
 20 know, is whatever activity we're doing compliant?
 21 Sometimes that's an easy call, sometimes it's a hard
 22 call, because many of the laws -- I'm most recently
 23 working in the telecommunications industry, and we have
 24 laws going back to 1934. So none of those laws even
 25 contemplated the environments we're living in today, so

1 you have to kind of read between the lines and figure
 2 out what you should be doing and what you shouldn't or
 3 what the intent of the law was.
 4 And then we have a lot of different
 5 self-regulatory groups, like the NAI and others, that
 6 focus on very specific, typically either activities like
 7 marketing or industry sectors. And I think it's a good
 8 balance, because the industry groups can move quickly
 9 when new issues surface or when new technology or new
 10 business practices evolve, and, if necessary, you can
 11 back them up with law on something that's really
 12 egregious or that industry is not able to get wide
 13 adoption for.
 14 So the risks, you know, most businesses today, I
 15 think certainly those that have any kind of
 16 international presence, with maybe the exception of some
 17 small ones, go through privacy impact assessments on
 18 what their business is involved in, and this -- and any
 19 assessment, you read any of the standard guidelines for
 20 a PIA, say you have to look at the risks and you have to
 21 mitigate those to the degree that it's possible or to
 22 the degree that it makes it acceptable, an acceptable
 23 level of risk, versus the benefit.
 24 MR. WOOD: Okay, great.
 25 Katie?

1 MS. MCINNIS: We know that businesses evaluate
2 the risks and benefits of data collection, but we also
3 know that they exhibit the normal human tendency
4 to overestimate the benefits of data collection in
5 comparison to the risks, and we have seen that through
6 many data breaches recently, that companies aren't
7 sufficiently internalizing the risk of all this data
8 collection when they evaluate the benefits of such
9 collection.

10 MR. WOOD: Great.

11 Bob, do you have -- as a cyber security expert,
12 do you have a different take?

13 MR. GOURLEY: Well, I would say that answers to
14 questions like this I think vary from industry sector to
15 industry sector depending on where you are at. For
16 example, in the financial sector, those companies are
17 all built around trust, especially if they are
18 consumer-facing, so they take an approach where
19 absolutely everything is evaluated from risk.
20 Compliance is critically important to them. Any heavily
21 regulated industry, compliance is extremely important.
22 We all know compliance does not equal security, and
23 compliance does not automatically reduce all risk of
24 data loss, but compliance is extremely important,
25 because if you fail, it can be a company-crushing event.

1 So I would say that my approach to questions like this
2 is to look industry by industry.

3 There are other industries where you're
4 collecting information that is already publicly
5 available. You're just pulling it together and using it
6 slightly different. So if that information is lost, is
7 that any risk? Does it hurt your brand at all if it was
8 all publicly available? And so the kind of question
9 like this, I think it's very important to figure out
10 what's the business model in the particular industry,
11 what are best practices for that industry, and then
12 what's the right approach.

13 MR. WOOD: Okay. So is reputational injury
14 important in advertising and privacy considerations as
15 well?

16 MS. FREUND: Oh, absolutely. That's why we're
17 here. I think, you know, what we represent is, you
18 know, people like Jennifer's former company and others
19 who came together recognizing that there was -- with all
20 of this data comes great power and great responsibility,
21 to use a Superman analogy, but I think that thinking
22 through -- it wasn't Superman?

23 MR. GOURLEY: Spider-Man.

24 MS. FREUND: Spider-Man, sorry. I have my
25 superheroes wrong. You can tell my kids are out of the

1 house already.

2 So I think that we have got a group of companies
3 that are dedicated to responsible data collection and
4 use practices because there's a need for that.
5 Consumers, you know, have said that there's a need for
6 that. Industry and regulators have recognized that
7 there's a need for that. There has been some talk of
8 legislation with no actual legislation enacted here in
9 the United States, at least, but we think about Europe
10 and the data protection legislation enacted there.

11 And so, yeah, I think in -- especially in
12 advertising, when you've got relationships with
13 consumers by first parties, but also the very backbone
14 of that advertising community is made up of companies
15 that are unknown to consumers, so it carries a bigger
16 responsibility. So because you're not necessarily known
17 to a consumer and you're collecting and using their
18 information, you've got to put certain safeguards in
19 place.

20 So we have lots of safeguards in place through
21 our self-regulatory code. Some of them I mentioned.
22 You know, as the data gets more sensitive, the
23 restrictions get more onerous. And so, you know, we
24 have, for example, a definition of sensitive data within
25 our code, and that covers a lot of some of the things

1 that were discussed in the earlier panels with respect
2 to health data. You know, some of those, as the
3 sensitivity increases, the requirements for what you may
4 and may not do with that data and the types of consumer
5 notice and choice that you put around that is really
6 important.

7 And so we base our code on the very basic
8 principles of privacy, on the FIPPS, and it centers
9 around notice, choice, accountability, and control. And
10 so in advertising, we think this is really important. I
11 think, you know, when it comes to, like I said, the use
12 of data to serve me a Nordstrom shoe ad -- just
13 hypothetically -- is less injurious to me than the
14 concept of somebody using, you know, something around
15 HIV status or gender identity.

16 So we've put guardrails around those things in
17 our code to try to make sure that folks understand that
18 they can trust -- I think trust in advertising -- and I
19 know a lot of what folks have mentioned on earlier
20 panels is the complexity of this environment, the data
21 environment. I'll use an analogy that is not my own,
22 but I'll use it anyway in terms of developing trust.

23 So you fly on airplanes every day, but you don't
24 necessarily know every word of what those mechanical
25 manuals say about how that airplane flies. You just

1 have to trust that the people that do know what they're
2 doing with it. And so part of our purpose and mission
3 is to hope that consumers will understand that people
4 that know this very complex digital advertising
5 ecosystem and the data that's around it will do
6 responsible things with it, and by adhering to our code
7 and the code of the DAA and other self-regulatory orgs
8 out there, we think that we, you know, are striking that
9 right balance between innovation and protection.

10 MR. WOOD: Okay. So do businesses -- I guess
11 you've addressed this, Leigh.

12 Other panelists, in your experience, do
13 businesses consider directly the injury to consumers?

14 MS. GLASGOW: I'm sorry, do they consider what?
15 There's an echo.

16 MR. WOOD: Sorry. Do businesses directly
17 consider the risk of injury to consumers?

18 MS. GLASGOW: I think they do, but I think it's
19 really difficult for them to understand what those risks
20 might be. Certainly the ones that I've been involved
21 in, whether it's Acxiom where I was an employee or
22 whether it was clients that we were serving, would ask
23 the question, what are the risks? And I think from this
24 morning's panel, if I hadn't said, either I as a privacy
25 officer for the company or the company themselves

1 probably would have not recognized over half of the
2 risks that were actually -- or the consequences that
3 were actually discussed this morning.

4 So I think there's an opportunity to continue to
5 educate the business community about how serious some of
6 these risks really are, because most of them, at least
7 in -- and I totally agree with Bob that it does vary to
8 sector to sector and how regulated or how -- what kind
9 of compliance obligations fall on the company, but
10 they -- it does -- it is one of those situations where
11 we need -- we need to understand all the potential
12 risks, and they're evolving.

13 We have new risks that surface, you know, with
14 new technology, and maybe the FTC, in conjunction with
15 industry, could do some more with that. IAPP, the
16 International Association of Privacy Professionals,
17 would be a great audience to carry those messages to the
18 businesses.

19 MR. WOOD: Okay.
20 Katie?

21 MS. MCINNIS: I just want to jump off of what
22 Leigh was talking about with the differences between
23 different kinds of information and the kind of
24 sensitivity we ascribe to them. I think that what's
25 getting complicated in this space is that with increased

1 data collection, nonpersonal identifying information is
2 now quickly becoming personally identifiable
3 information. So although you may not know my gender
4 identity, you may know what kind of products I'm looking
5 for online, and therefore can make an inference that I
6 have this gender identity. Or maybe you don't know my
7 HIV status but you know that maybe I'd be in the market
8 for an at-home test. So it does get very concerning,
9 this huge collection of data and the kind of inferences
10 you can draw from it, and I think we need to be aware of
11 the kind of data that you're collecting can really be
12 highly sensitive even if the individual data points
13 don't seem sensitive on their face.

14 MR. WOOD: And do you think businesses are
15 inadequately aware?

16 MS. MCINNIS: I think it's hard to tell. I'm not
17 a business. I haven't worked for a business. So that's
18 a little hard for me to tell personally, but I do know
19 that with the number of data breaches that have
20 occurred, especially in industries that do not have a
21 direct relationship with consumers, Equifax is a great
22 example, we know that there's a huge amount of data
23 about individuals that they never really opted in or
24 gave permission to be collected about them, but it can
25 have a really injurious effect on their livelihood and

1 also some clear informational injuries beyond just
2 financial injury.

3 MR. WOOD: Okay, great.

4 MS. FREUND: Could I quickly respond? Oh, sorry,
5 Jennifer had her card up.

6 MS. GLASGOW: Yeah, I want to make a point that I
7 think we need to think about data breaches in one light
8 and then we need to think about inappropriate use of
9 information by the company in another light, because
10 both of them can be harmful, and quite often we conflate
11 the two, and I think resolution and mitigation for those
12 kinds of bad practices may differ dramatically between
13 the two categories.

14 MS. FREUND: Yeah, so Jennifer took my answer.

15 MS. GLASGOW: Sorry.

16 MS. FREUND: But I will add to that that I think
17 the concept that Katie rightly brings up is, you know,
18 what data do you need to do the action that you are
19 doing? You know, the less data you have, obviously,
20 the -- the less risk of data breach, and I agree that we
21 need to keep them kind of separate and distinct, but,
22 you know, in our case, advertising data is only valuable
23 in very limited circumstances and for very limited time
24 periods, so one of the things we counsel our companies
25 or our members to do is, you know, practice very good

1 data minimization. So if you don't need the data and
2 you don't need it any longer because the person's bought
3 the car or bought -- in my case bought the shoes -- you
4 know, get rid of it.

5 So that is something that I think, you know, good
6 data responsibility and good data collection practices
7 and use will -- will engender that concept of data
8 minimization, and I think it's important.

9 MR. WOOD: How -- how -- do businesses in general
10 seem like they're cognizant of data minimization and how
11 important it is?

12 MS. GLASGOW: I think they're aware of it.
13 Again, it is going to vary with the industry and it may
14 also vary with the size of the company. It's something
15 that they talk about. If there's any kind of
16 international footprint, because those are more
17 regulated kinds of activities in other geographies, it
18 becomes more important to them, because they know it's
19 important in Europe, and it's easier to just deal with
20 it worldwide than it is to do things differently in one
21 country from another.

22 So -- but I want to caution against data
23 minimization being too much of a panacea. It's --
24 knowing how long you need the data and how long it's
25 useful is important, but some data has a lifetime of

1 the future, and they're moving a lot faster than I
2 believe the government or even consortiums can, and
3 they're adopting things like very smart encryption, ways
4 to stripe and secure data and spread it around places
5 where it's harder to penetrate, not perfect, but harder.
6 They're also advancing cryptologic concepts called,
7 like, differential privacy. Have you guys heard of
8 differential privacy? It's a cryptographic construct
9 that has been around for several years. It was now
10 brought into Apple's iOS 10, so we are all using
11 differential privacy now, didn't even know it. It's in
12 Apple. Facebook is using it. Google is using it. What
13 it does is it allows you to extract data from data sets
14 in ways that do not reveal the underlying data but give
15 you statistically meaningful information. A simple way
16 to think of it is when you use the traffic on your
17 Google Maps and it says that it's red on this road, it
18 knows that because they're watching the traffic, and
19 they do that in a way that does not take away the
20 privacy of the individuals and how slow they're moving.
21 So my bottom line point to all this, watch GAFA. Watch
22 where the big guys are going with privacy and protecting
23 data. I think it's extremely important. So the
24 question to ask yourself, what would GAFA do?

25 MR. WOOD: Okay. So we've heard that various

1 value, and so, you know, the idea that all data has an
2 expiration date that's fairly short I think may lead you
3 into a situation where you're not maximizing the benefit
4 you could bring to it.

5 For instance, if you want to contrast marketing,
6 which as Leigh has said, has a much shorter lifetime of
7 value, to identity theft, where if I have a pattern of
8 where you've lived for the last 20 years, I can do a
9 better job of predicting that you are the person you
10 claim to be than if I have two years of that data. So
11 it can be very variable.

12 MR. WOOD: Okay.

13 MR. GOURLEY: I would like to push on that just a
14 little bit, too, and say I have not seen a correlation
15 between how much data you have and the likelihood that
16 it will be breached. Your data needs to be secure even
17 if it's a very small pile of data, and a lot of times a
18 small pile of data in a small company is actually of
19 greater likelihood of breach because that small company
20 can't protect it as well. I would say what would GAFA
21 do? We have got to watch what GAFA is doing, because
22 they are leading us all forward. Who is GAFA? What's
23 GAFA? GAFA is the big industry players when it comes to
24 data. Google, Apple, Facebook, and Amazon. GAFA is
25 leading us all into how we are going to do privacy in

1 factors businesses take into account in thinking about
2 the risks and benefits, so maybe GAFA, the trust that
3 the consumers are placing in them, consumer
4 expectations, compliance, and regulatory issues, and
5 sometimes direct the sort of concrete injuries possible
6 to consumers.

7 How well do these factors businesses consider
8 correlate with potential injury to consumers?

9 MS. FREUND: Could you --

10 MR. WOOD: So how well do the various factors
11 businesses think about when they're weighing whether and
12 how much data to collect and share correlate with the
13 potential injury to consumers?

14 MS. GLASGOW: I'll start it off. The -- I think
15 this is where I want to answer it -- answer the question
16 first for -- from a security breach perspective and then
17 from an appropriate use of data perspective.

18 From a security perspective, I think they
19 correlate pretty well. We're now looking at all kinds
20 of security related to data at rest, data in transit,
21 and so on. So -- and to pick up on the GAFA analogy,
22 the fact that we're using cloud computing, where many of
23 the security precautions that a small company would
24 never be able to put in place are made available, is
25 actually a really positive step forward on the security

161

1 side of the house.
 2 Now, that doesn't help at all with, you know,
 3 internal use of information and whether it's
 4 appropriate, and I think that we're beginning to realize
 5 that as data becomes part of every business practice,
 6 regardless of what it is, and much of it is personal
 7 data, whether it's anonymized or not, it -- it has both
 8 opportunities and risks, and those need to be evaluated
 9 as carefully as possible.
 10 I used to say that, you know, we could put some
 11 guidelines out there, whether they were self-regulation
 12 or legal guidelines, that governed or they gave
 13 companies guidance about what they should and shouldn't
 14 be doing, but as information has proliferated,
 15 everything we do and the opportunity, the analytics that
 16 we have to turn it into valuable insights, it gets very
 17 easy to do, not just -- not just available to large
 18 companies with sophisticated data scientists.
 19 We have surfaced a different issue, and it is
 20 every single use of data in a company needs to be looked
 21 at through the lens of a privacy impact assessment, and
 22 that should include the risk to the individual as best
 23 they can assess them. I -- in work -- if you look at,
 24 say, an industry such as the risk side of the house
 25 where you're doing identity verification to try to

162

1 understand if you're dealing with legitimate people or
 2 may be required by law, as it does with
 3 Gramm-Leach-Bliley, where there's a know your customer
 4 rule, to actually verify that you're dealing with who
 5 you think you are, those are industries that really pay
 6 a lot of attention to these kind of issues.
 7 I find that some of the tech industries and some
 8 of the startup industries are not as consistent, if you
 9 will, in their evaluations of the internal uses of data
 10 outside of security.
 11 MR. WOOD: Katie?
 12 MS. MCINNIS: Data security should be in line
 13 with what a consumer expects and the the business is
 14 really putting a high priority on; however, the number
 15 of data breaches we've seen even just in the past five
 16 years show that that isn't significantly guarded, right?
 17 We have Aetna, Uber, Yahoo, Equifax, so many companies
 18 have not sufficiently protected the data that they were
 19 entrusted with from consumers, and that's highly
 20 concerning, and that should be their priority, and
 21 that's what consumers expect, yet we're not seeing that
 22 being fulfilled.
 23 And as far as misuse of data or privacy of
 24 consumer data, we're also seeing that that's not
 25 necessarily a priority. One good example is Uber's

163

1 recent breach, right? They had a breach. They worked
 2 to cover it up. And then they also misused some
 3 internal data in ways that consumers felt was really,
 4 really creepy, and led to some changes in their
 5 policies.
 6 We see that change in their policies because they
 7 are consumer-facing and they depend on the consumer
 8 trust. So, yes, both of these things should be
 9 important to companies, especially data security, but
 10 we're not seeing sufficient protection of either.
 11 MR. WOOD: Okay.
 12 Leigh?
 13 MS. FREUND: Yeah. So just a couple quick
 14 things. I mean, one is when we think about our industry
 15 in general, I think, you know, it's important to kind of
 16 keep in mind that without the consumer clicking on an
 17 ad, you know, none of this is here and none of this
 18 works. So obviously keeping the consumer kind of top of
 19 mind as we go through these processes is important,
 20 whether or not we do it enough is a matter for debate,
 21 but -- and I do think it's important to think about, you
 22 know, Jennifer mentioned, you know, it's harder for some
 23 of the smaller companies, the startups and the smaller
 24 tech companies to kind of put privacy top of mind due to
 25 either resource constraints or other things, and I will

164

1 say, you know, just a little plug for us that the
 2 compliance process that we undertake with our member
 3 companies, big or small, is the same process for every
 4 company, every year, on an annualized basis, and it
 5 helps make them put a priority on privacy that wouldn't
 6 otherwise be there, and I think, you know, we have --
 7 Anthony, my compliance person -- VP is sitting right
 8 here, and he can tell you the rigorous and onerous
 9 process that folks go through, but I think it's
 10 important to think, when you think about consumers and
 11 putting them at the corner stone of things, priority --
 12 the priority of privacy becomes really important, and so
 13 we build things around it that help us, you know, make
 14 sure that even the smaller tech companies and the
 15 startups put priority -- put a priority on privacy.
 16 MR. WOOD: Okay, great.
 17 MS. HAN: Great. Thanks. So, Leigh, I want to
 18 build on something that you just said, putting consumers
 19 sort of at the front of mind, and my question for you
 20 all is do businesses think consumers are informed about
 21 the benefits and risks to consumers from collecting and
 22 using their personal information?
 23 MS. FREUND: Yeah, I think that is something that
 24 folks will probably disagree with on -- even among our
 25 panelists here, but I think, you know, one of the things

165

1 that we -- we do, at least for our industry, is make
 2 sure that our members are aware that one of the
 3 cornerstones and pillars of ourself-regulatory program
 4 is consumer outreach and education. That's part of what
 5 they're required to do as part of our compliance
 6 process, et cetera.
 7 So we try to make -- you know, through either our
 8 own organization's efforts or through our member
 9 companies, try to make consumers aware of the fact that
 10 they do have choices about what happens with their data
 11 and try to bring folks to our website where they can
 12 learn more about what this digital advertising is, why
 13 am I being targeted, why is this ad following me around.
 14 We have some educational, you know, components of our
 15 website that try to help people understand that a little
 16 bit more and help understand what the options are, if
 17 they choose to exercise them.
 18 I think, you know, in general, we have found,
 19 through some research, that consumers are pretty -- are
 20 becoming more aware. I think this is where
 21 self-regulation has an advantage over some of the
 22 other -- the other types of things that we could do,
 23 like regulation or legislation, because we can respond
 24 to things a little bit more flexibly and quickly as new
 25 technology is developed, but I think consumers'

166

1 expectations are also evolving in this area quite a bit.
 2 You know, I think about, you know, what we know and
 3 understand in the industry, but also about, you know, my
 4 parents living in Michigan, who didn't grow up with this
 5 technology -- I think they're listening, hi, mom and
 6 dad -- and what their expectation is might be completely
 7 different from the folks living in Silicon Valley or the
 8 folks living here, working in this industry.
 9 So it's really incumbent upon the companies to
 10 try to use those efforts to make sure that they are
 11 understanding -- that they're trying to educate the
 12 consumers about what their choices are and what type of
 13 data they use. I mean, privacy policies, we can argue
 14 that those aren't necessarily as informative as perhaps
 15 they should be, because they're buried, but trying to
 16 think of proactive ways to make consumers informed is
 17 really important, at least to our companies.
 18 MS. HAN: Thank you.
 19 Omri?
 20 MR. BEN-SHAHAR: Yeah, I would like to take an
 21 issue with that. I think I'm deeply skeptical about
 22 education, transparency, privacy policies. It's a nice
 23 kind of thing for the companies to brandish and for the
 24 law to require, but it has no effect whatsoever. We
 25 know that for a fact from numerous studies, and there is

167

1 no way to make it work either, in part because we have
 2 to realize we're sitting here talking about privacy, but
 3 there are panels around the country and around this city
 4 and around -- where people are talking about other
 5 aspects of the consumer transaction that consumers care
 6 and some law makers and some advocates care not less
 7 than data privacy, for example, the choice of forum, the
 8 arbitration clauses, and the ALI cares a lot about the
 9 warranty disclaimers and the way laws are being
 10 completely disclaimed by the -- so it's hard to educate
 11 consumers about everything and especially about, I
 12 think, data policy, because it's a moving target. It
 13 advances so fast that by the time people catch up, they
 14 are already two or three years behind.
 15 That said, you know, I would think that if --
 16 that doesn't mean consumers don't largely understand
 17 what's going on. I think maybe they -- there is some
 18 indication that they do. I don't want to -- I can't say
 19 that as a fact, but that they -- people say in surveys
 20 that they are concerned about what's going on. That
 21 means that they think that the data collection and data
 22 usage and sharing is done in ways that they can't
 23 pinpoint the details, and they will not be able to
 24 understand, but it causes them to -- them concern. So I
 25 think that there is a sense of the risks that comes

168

1 maybe from experience and from some other contexts, not
 2 from privacy policies.
 3 The other thing that I want to say about that is
 4 that I think consumers view -- return to that basic
 5 point, that consumers view data policy as one aspect of
 6 the transaction. The data collection and practices of
 7 firms is -- in part, consumers view it as a good thing.
 8 Privacy or information is the new money -- I've said
 9 that before -- and people are delighted to pay with
 10 information rather than with money. I mean, they
 11 probably would prefer to do neither, but I think that
 12 there is a general understanding as well that there is a
 13 grand bargain here where information becomes the
 14 currency.
 15 Also, personalized services are largely good.
 16 People enjoy them. There's both a private -- a great
 17 private benefit. I mean, this is a symposium about
 18 informational injury, but I think from a social point of
 19 view, we really also want to think about informational
 20 benefits. There are -- Catherine Tucker, who sits here
 21 and will talk later, did some work about the value of
 22 personalized service, about digital medical records and
 23 the life-saving effects that they have.
 24 I've looked at some work that is basically -- you
 25 know, digital records and data collection in the auto

169

1 insurance industry and these pay-as-you-drive
 2 arrangements that are, by the way, prohibited in places
 3 like California because of privacy concerns, and the
 4 value that they can bring, under some estimates it could
 5 be as much as 20 percent reduction in accidents. When
 6 the insurance company knows how you drive and when you
 7 drive and how much and where and how abruptly you stop
 8 and things like that, and it changes the premiums
 9 accordingly, that may be a privacy issue, but it also
 10 leads people to drive in a safer way. One estimate that
 11 I saw is a reduction of up to 20 percent in auto
 12 accidents. That's, like, 3000 lives a year, I don't
 13 know, maybe more. That's -- there must be a very large
 14 privacy concern to override that benefit, and I'm not
 15 even talking about the fact that people whose
 16 pay-as-you-drive habits are measured, drive less, and
 17 another estimate is about 8 percent less, and that is a
 18 reduction equivalent -- that's an enormous reduction
 19 equivalent to about \$1 of carbon tax, so there is an
 20 environmental benefit.

21 There is also a benefit here to low-income
 22 drivers. They usually drive less, so they will get
 23 lower premiums. All of that stuff comes -- are benefits
 24 that come from data collection that the consumer, if
 25 they enjoy them, are enrolling into. They like these

170

1 things. That's the context of what the people realize.
 2 Of course, there are the bad things that people
 3 are not -- either not aware of or when these things hurt
 4 them, and I can't say that this is considered by
 5 consumers as worse than other "fine print things," like
 6 termination fees in cell phone contracts or warranty
 7 disclaimers or things like this.

8 So consumers are -- to wrap up, consumers are
 9 aware that this thing is going on. They are not aware
 10 of the details and how advanced some of the collections
 11 are, but not concerned enough to buy privacy shields
 12 that are not that expensive and to protect themselves
 13 from these things.

14 MS. HAN: Thank you.

15 So this is a great transition for us into sort of
 16 the consumer perspective and how consumers weigh the
 17 risks and benefits in determining how to share their
 18 information. So, Jennifer and then Katie.

19 MS. GLASGOW: Yeah, I'd like to pose that we
 20 have -- consumers have things they expect to happen, and
 21 I think security certainly falls into that category. We
 22 don't give them a choice about security. That's a
 23 must-do. Whether we do it well or not is, you know,
 24 something we can debate.

25 But then there are things that we should give

171

1 consumers choice about, a la, online advertising, as
 2 Leigh's organization has put forth, but I tend to be a
 3 bit skeptical about their understanding, and I think we
 4 need to separate notices and policies from
 5 understanding.

6 I've been knocking around this information
 7 world -- I started out on the technical side of the
 8 house many, many years ago, and I find that even as a
 9 professional in it, it's sometimes very tedious for me
 10 to understand what-all is happening, and I think as we
 11 move into more big data applications and more analytics,
 12 where decisions are being made by the analytics engine,
 13 it's going to get even harder.

14 So I feel like we're going to have to get
 15 industry to rally around setting guidelines, like the
 16 marketing and digital advertising industry has, that
 17 industry has to follow and that we don't have to ask the
 18 consumer a choice about, because there's a lot of
 19 research that shows that when consumers are given a
 20 choice, if they aren't sure about what they're really
 21 being asked, they take no action. So that means the
 22 default becomes extremely important in terms of is this
 23 going to be something that's allowed or is this going to
 24 be something that happens and they have an opportunity
 25 to stop?

172

1 MS. HAN: Thanks.
 2 Katie?

3 MS. MCINNIS: So I do think that there is an
 4 understanding that consumers have. To a certain extent,
 5 they are trading information for a free service. I
 6 think people do generally understand if they sign up for
 7 Facebook, they're trading a certain amount of
 8 information away in order to use this free social
 9 platform.

10 However, I don't think that that's always the
 11 equation here, especially when you have a number of
 12 unknown data brokers and other companies online that are
 13 collecting my data at a rapid rate. I have no
 14 understanding that I'm getting anything from them by
 15 their collection of my data, nor is there any benefit to
 16 me.

17 And I also want to challenge the assertion that
 18 people want personalized services. Yes, to some extent,
 19 I would benefit from personalized services from some of
 20 the organizations and companies that I interact with,
 21 but on the whole, I do not want targeted ads across my
 22 web service, which is why I'm one of the many users of
 23 ad block services.

24 And the increased use of ad block services is
 25 showing that people do not really want this supposed

173

1 personalized service that we so think they want. The
 2 personalized service also is clearly not about me but
 3 about making revenue on the other side, and I think
 4 consumers do understand that.
 5 And as far as how much consumers are
 6 understanding the kind of disclosures they agree to, I
 7 agree it's incredibly hard, and there is a lack of
 8 complete understanding, in part because a lot of it's
 9 happening on the back end, which is why you have even
 10 like Facebook that does a lot of work to make sure that
 11 you know what kind of people are seeing your data.
 12 People are still asking if Facebook is listening
 13 to them. So there is this -- this gap of understanding
 14 of, oh, I have a lot of contacts, and, therefore, that's
 15 why they're recommending a client that I saw last week
 16 on Facebook.
 17 So there is this gap in understanding, and I
 18 don't think we should really always put that on the onus
 19 of consumers, right, and that's one reason why other
 20 intermediaries like Consumers Union is here to try to
 21 help evaluate the kinds of policies and disclosures that
 22 are out there and help consumers decide which companies
 23 and products to use.
 24 MR. WOOD: Any other comment?
 25 MS. HAN: Leigh, then Bob?

174

1 MS. FREUND: Bob, please go ahead.
 2 MR. GOURLEY: First of all, just like so many
 3 other people, I love Consumers Union. I'm so glad that
 4 you guys are doing what you are doing because we all
 5 need that. And I also want to say that I feel ignorant
 6 after studying these things for decades, and I realize I
 7 don't have a full understanding of what it means when my
 8 data is breached and lost.
 9 Sometimes I get angry and I know it's wrong, like
 10 the OPM breach, stealing my data, that was bad,
 11 horrible, but it had no real cost to me, or the Equifax
 12 data breach, I got angry like 190 million other people
 13 because the data is out there, but as I thought about
 14 it, I realized that had zero impact on me. I locked
 15 down my all credit records anyway. It had a big impact
 16 on that company, because they are in the business of
 17 selling my data, but that's not my business. It didn't
 18 hurt me at all. My data had already been stolen, and my
 19 Social Security number is out there. Why? Because I
 20 was in the Navy, and every year that I got promoted, it
 21 was in the Congressional Record, here's Bob Gourley,
 22 this Social Security number, achieves this rank. So
 23 with that data being stolen, it has zero impact on me.
 24 So how am I supposed to quantify that? And for me, I
 25 don't want any of my data stolen, but I have no way of

175

1 understanding, if there's a big breach, what the cost to
 2 me is. I do want my privacy protected like everybody
 3 else. I mean, what I do is my business, but I just -- I
 4 am not quite sure how to quantify or put a number on the
 5 impact of a breach.
 6 MS. HAN: Thanks.
 7 Leigh?
 8 MS. FREUND: Yeah, I just wanted to touch quickly
 9 on the ad blocking issue. You know, folks that don't
 10 want targeted advertising, you know, many of them
 11 download ad blockers which actually block the
 12 advertisements that are on your site in general. You
 13 know, I would say the answer to that is go to the NAI
 14 website and exercise your opt-out, but I will say that
 15 we've done a lot of work through some coalition building
 16 in our industry on the concept of ad blocking, and we're
 17 realizing that privacy is not the top reason that people
 18 are downloading ad blockers.
 19 It's not that they don't want targeted ads. It's
 20 that they don't want their data to be used. It's that
 21 they don't want a terrible user experience. And I'll
 22 suggest that, you know, when we use targeted or
 23 behavioral advertising and try to use data minimization,
 24 to not use as much data as we need to do that, but that
 25 it actually creates a better online experience for

176

1 users, you know, to get the same economic value out of a
 2 targeted ad. When you're not using data, you would have
 3 to have 20 popovers, 20 popunders, and some flashing
 4 jiggly belly ads on the page in order to try to make up
 5 that revenue for the publisher.
 6 So ad blocking is harmful to that kind of
 7 continuation of free content and services on the
 8 internet, and the reason people are using it is not
 9 necessarily privacy-related. Although it is one of the
 10 reasons, it is kind of down the list.
 11 MS. HAN: Katie?
 12 MS. MCINNIS: I just wanted to touch on something
 13 that Bob highlighted, which is these injuries to
 14 consumers are highly contextual, right? You have an
 15 incidence in which OPM, an organization you knew about
 16 had your information, was breached, and you already knew
 17 about this and, therefore, acted proactively and froze
 18 your credit reports with the three major credit bureaus,
 19 which is great.
 20 However, for a lot of people -- first of all,
 21 they didn't have a relationship with Equifax, so they
 22 were surprised not only that their data was breached but
 23 also weren't really sure how to handle it; and secondly,
 24 now they had to go take the step you did a while ago,
 25 and, therefore, they don't know what kind of future

177

1 injuries could happen to them, in addition to the fact
 2 that a lot of this information is immutable, like a
 3 birth date, et cetera.
 4 So the injury maybe hasn't happened now and it's
 5 hard to quantify, but it could happen in the future,
 6 which is one reason why it's so hard, especially for
 7 regulators and other organizations, to really analyze
 8 and understand what kind of injuries these cause to
 9 consumers because it is so highly contextual.
 10 MS. HAN: Omri?
 11 MR. BEN-SHAHAR: Yeah, thank you. I'd like to
 12 touch on some of these issues that Katie raised. I
 13 think that, you know, it's -- the question to ask all of
 14 us, what I said and others, what do people care about?
 15 You know, I think that that's the key issue, not what do
 16 people say they care about, but what do they actually
 17 know when they are -- when there are stakes on the line,
 18 what do they care about?
 19 It really shouldn't -- I don't think the FTC
 20 should listen to privacy advocates or privacy skeptics,
 21 to alarmists or deniers on either side about saying,
 22 hey, I download ad blocker. People -- you know,
 23 that's -- you know, we are not representative of
 24 anything.
 25 Also, I don't think that the FTC should listen

178

1 very much to what people say in surveys they care about,
 2 because they will say they care about anything, you
 3 know, and there's a lot of things that just don't add
 4 up. The question is, what do their behavior shows when
 5 there are stakes -- real stakes on the line, when they
 6 have to make hard choices, what to spend money on or
 7 what to sacrifice or what burden to take, what kind of
 8 ads -- popping ads and all sorts of these things,
 9 flashing, nonpersonalized ads, to suffer through?
 10 So as to not be personalized, then maybe they
 11 will say, you know what, maybe I don't care about it
 12 that much. I think these are the questions that
 13 determine whether there is an injury in a sense that is
 14 meaningful. Otherwise, it's all kind of arm-waving
 15 about either, you know, people -- either biased people
 16 that do not represent anyone or people say things
 17 because, you know, the context they were asked.
 18 They say, oh, yeah, by the -- since you asked
 19 about data sharing, sure, I care about it. You know,
 20 what does that mean?
 21 MS. HAN: Okay. So I wanted to build on both
 22 Omri's and Katie's comments. Oh, actually, Katie, did
 23 you want to --
 24 MS. MCINNIS: Yeah, I just wanted to quickly
 25 respond, if that's okay.

179

1 MS. HAN: Sure.
 2 MS. MCINNIS: Yeah, I take your point that survey
 3 data isn't indicative of what a consumer's actually
 4 going to do, and I hear your logic behind that, and I
 5 just want to counter that maybe there's something else
 6 going on here. Maybe consumers just don't feel like
 7 they have the tools to effectively make sure that their
 8 preferences are appreciated across many devices and
 9 services they use, which is one of the reasons why the
 10 FTC launched their IOT -- their IOT contest last year,
 11 was to try and come up with a way that consumers can
 12 control the different devices and services they use
 13 within their home to make sure their preferences are
 14 respected across platform and device.
 15 I think that consumers feel like they don't have
 16 a lot of tools, which is -- to be fair, the industry is
 17 hugely fragmented. These policies are really, really
 18 long and hard to compare, and even when you are in the
 19 market for a privacy protective service, like a virtual
 20 private network, it's sometimes hard to know what kind
 21 of services you're actually receiving, and CDT's recent
 22 work and complaints to the FTC highlight that.
 23 Even if you're presented with these assertive
 24 statements of what is going to be protected, you're
 25 really unsure if that's actually going to be followed

180

1 through on the back end, and that's one reason why these
 2 policies and privacy statements are so important, is
 3 because that's in some ways the only way we know what
 4 companies are doing with our data and information and
 5 the only way to effectuate those choices.
 6 MS. HAN: Thanks.
 7 So I wanted to back up just a second because Omri
 8 and Katie both talked a little bit about context, and I
 9 wanted to give the other panelists -- and also them, if
 10 they have additional thoughts -- to weigh in about how
 11 the context or kind of data being shared matters when
 12 you're thinking about how consumers are making those
 13 decisions.
 14 MS. GLASGOW: Do you want me to start?
 15 MS. HAN: Go ahead.
 16 MS. GLASGOW: I don't think, other than just
 17 sharing sounds scary, I don't think most consumers
 18 really think about it, because I don't think they
 19 understand it. Data sharing goes on in all kinds of
 20 ways in every industry. I mean, if I think about the
 21 doctor sharing data with a specialist they've sent me
 22 to, and they send your regular medical records over or
 23 whatever, and every industry has a different kind of
 24 sharing practice.
 25 It may be with a third party who's out -- you've

181

1 outsourced work to. It may be with a delivery service
 2 that's going to deliver the product to the consumer. I
 3 mean, it goes on all the time. So there are some things
 4 that the consumer touches and feels and understands,
 5 that FedEx is going to see the package that I ordered
 6 from Amazon or wherever, but when it comes to what goes
 7 on behind the scenes, I think they are pretty clueless.
 8 MS. FREUND: Yeah, if I could add on to that, I
 9 would just say, you know, I think that consumers
 10 probably have a different understanding. I think, you
 11 know, when we get consumer complaints to our site, you
 12 know, we get, you know, I got a targeted ad, stop using
 13 my Social Security number.
 14 You know, so the concept of what kind of data
 15 people have, I think the "sharing is scary" comment is
 16 really important, because I think consumers feel like,
 17 you know, for instance, if you get a targeted ad, you
 18 must know my Social Security number, my address, my
 19 credit card, and my Nordstrom frequent shopper card
 20 when, you know, really it's a binary decision made by
 21 usually an algorithm that says, do I serve this consumer
 22 this ad or this ad?
 23 And when you're talking about the concept of
 24 injury, you know, on top of that, I think it's important
 25 to remember, you know, consumers -- and I think it's

182

1 important to try to continue to educate consumers as
 2 much as we can, but I think that's where the airplane
 3 analogy that I used earlier and the trust factor kind of
 4 factors in. If you're on a website or using a provider
 5 that you trust or that you feel like you can exercise
 6 your own choices with respect to that, then you're going
 7 to have trust and you're not going to have to understand
 8 the complexity of the ecosystem to feel like your data
 9 is safe. And security I know weighs into that very
 10 heavily, so...
 11 MR. GOURLEY: Yeah, we can talk about that, too.
 12 The security piece, depending on what your business is,
 13 there is already security architectures in place to
 14 exchange data securely with consumers, especially in the
 15 finance world. You know, if you have done a mortgage
 16 recently, you have to get documents to your mortgage
 17 provider. There's secure ways to do that.
 18 In my business, we used to do a lot of work by
 19 email. There has been a big shift in business recently
 20 towards very secure channels -- Signal, Telegram, Wicker
 21 are key providers with secure capabilities -- where you
 22 make sure that nobody can eavesdrop on your business
 23 chatter or communications with other businesses. I
 24 think that's going to grow significantly and begin to
 25 reach into consumers, too.

183

1 So the consumers won't have to share information
 2 by email, which is really vulnerable unless you're using
 3 a big provider like GAFA. GAFA does secure email. I
 4 trust Google, Amazon, Facebook, Apple, when it comes to
 5 email, but other than GAFA, if you are using any other
 6 provider, it's unsecure.
 7 And so you're sharing information with a company.
 8 That company is storing it in some server somewhere, and
 9 it could get breached or lost or, you know, some
 10 employee could hit a button and send it to someone else.
 11 There's great room for new architectures and new
 12 solutions that will improve consumer privacy and protect
 13 business information through these secure solutions,
 14 like Wicker.
 15 MS. HAN: Thank you.
 16 MR. WOOD: So we've been on this topic for a
 17 little bit, but what other obstacles do consumers face
 18 in evaluating the benefits, costs, and risks of
 19 information sharing?
 20 Omri?
 21 MR. BEN-SHAHAR: Well, I think the main obstacle
 22 is complexity. Everything in the consumer world is
 23 complex, not just data policy. I mean, you can make
 24 things really simple for consumers if you really wanted
 25 choice, you know, every app, every website could have a

184

1 very clear button, "Do not track. Shut down all data
 2 collection and everything." That would make things very
 3 simple on the face of it, but, of course, it's not,
 4 because many other elements of the transaction depend on
 5 the fact that these businesses can harvest information
 6 and provide some -- sometimes it's for functionality,
 7 other times for profitability and the cost of the
 8 service, and now you have to -- if you shut down the
 9 data collection, if the consumer simply clicks that
 10 button, other things pop up.
 11 Well, actually, now you have to choose. Do you
 12 want the premium or -- version, how much you want to
 13 pay, things like this? There is no way around the
 14 complexity of this aspect.
 15 And then once you throw in that every one of
 16 those consumer transactions has other elements that --
 17 as I mentioned, other audiences, not in this room today,
 18 but think -- other audiences think they are the most
 19 important ones, and the democracy depends on them, like
 20 class action waivers, arbitration clauses, and the like.
 21 Then, you know, you have -- how many buttons do
 22 you have to give consumers to click and unclick and how
 23 often do they have to do it, because every website and
 24 every app has to have this. So, you see, it's becoming
 25 an infinite task of choice, and I think any reasonable,

1 emotionally sound, and rational consumer would say,
 2 "Please don't burden me with this world of autonomous
 3 choice."
 4 MR. WOOD: Jennifer?
 5 MS. GLASGOW: Yeah, I just -- I totally agree and
 6 I would like to add two more factors to the what do they
 7 understand. One is, it is constantly changing. A
 8 company that didn't have good security practices may
 9 have decided that they wanted to go use AWS and is now
 10 under very good security practices. So the fact that a
 11 situation -- you make a decision at a point in time to
 12 either do something or not do something, you might want
 13 to re-evaluate that on a fairly frequent basis.
 14 The other piece I'll put on the table, which I
 15 think is going to be more and more prevalent in the
 16 coming years, is the whole idea of big data and very
 17 analytically driven business models, where it is the
 18 computer that's making the decision. And we obviously
 19 have seen a lot of that in the health area, and it's
 20 fabulous results. We see it in cities. We see it -- we
 21 see it in advertising. We see it in everything we
 22 touch.
 23 But I think it's going to make it harder and
 24 harder for the consumer to understand how you went from
 25 point A to point B, and I will give an example that goes

1 back many years. There has been a very, very high
 2 correlation between insurance claims and your
 3 creditworthiness, and across the states, many of the
 4 states, the legislators did not understand that
 5 correlation.
 6 Whether or not the industry did a good job of
 7 explaining it, I can't say, but they didn't understand
 8 the correlation. So many, many states have passed laws
 9 that restrict the use of credit information relative to
 10 insurance claims. And so that is a valid statistical
 11 piece of information that would help. It may not help
 12 an individual who has bad credit, but it would certainly
 13 help those that do to differentiate good practices from
 14 bad practices, but we're barred from doing it today by
 15 law. So that's what you've got to be careful that you
 16 don't -- the trap that you don't step into.
 17 MR. WOOD: Katie?
 18 MS. MCINNIS: So as far as consumer obstacles in
 19 this space, we've talked about the law and policies and
 20 how it's difficult for consumers to evaluate those.
 21 We've also discussed the difference between a
 22 consumer-facing organization and an organization that
 23 has no direct relationship with a consumer, where there
 24 really isn't this array of opt-in or opt-outs even
 25 available to the user. So those are two huge obstacles

1 to consumers.
 2 Another one is that they really do have a hard
 3 time prioritizing future risk of disclosing this
 4 information when they're facing immediate problems
 5 setting up a new device or a new service that they
 6 really want the service from.
 7 I think part of that is also due to the relative
 8 immaturity of our market. IOT devices offer a huge
 9 amount of functionality to users, and they definitely
 10 want to take advantage of that, but a lot of times they
 11 are not able to even assess the security or privacy
 12 concerns within those devices or adequately assess the
 13 privacy policies as compared to another device, which is
 14 one reason why Consumers Union/Consumer Reports,
 15 launched our digital standard last March to begin
 16 evaluating products and services under privacy and data
 17 security, but also in connection to the kind of services
 18 that these products can provide to you.
 19 So I may be wanting a new TV and I will be able
 20 to assess the kind of color and richness and use of the
 21 TV, along with the security and privacy of these TVs,
 22 and compare that to other models, and that really does
 23 allow the consumer to effectuate some choice, where
 24 we're taking into account not only the service of the
 25 product but also the kind of data and privacy security

1 concerns.
 2 MR. WOOD: Omri?
 3 MR. BEN-SHAHAR: I want to say this, maybe I will
 4 pose it as a question to Katie, but my impression is
 5 that there are services in the market, when we had
 6 Professor Alessandro Acquisti here from Carnegie Mellon,
 7 so Carnegie Mellon, nonprofit, made an effort to rate
 8 the privacy performance of mobile apps,
 9 privacygrades.org, and this information is all boiled
 10 down to a single score, and yet I don't have the
 11 impression -- again, maybe I'm wrong -- that consumers
 12 are, you know, swarming to privacygrades.org to get
 13 that.
 14 If these kind of efforts are failing, what does
 15 this tell us about the underlying question that we are
 16 all sitting here today to discuss, which is what is the
 17 consumer's injury from the existence of these practices?
 18 MS. MCINNIS: I don't think that we're failing.
 19 I think that we're really just trying to catch up. Bob
 20 pointed out that a lot of these tech companies are
 21 moving much faster, and I think Leigh and Jennifer also
 22 mentioned this as well that tech companies are moving
 23 far and beyond faster than regulators and other kinds of
 24 checks and balances on this industry are, and that
 25 unfortunately is just how it is so far, but we're trying

1 really hard to catch up.
 2 And just evaluating the privacy and security of
 3 apps to me doesn't create a full picture, right? Even
 4 if I know that this might have bad privacy and security,
 5 I'm only using it for some limited use, so I might not
 6 really care; however, something that has more personal
 7 information or affects my everyday life, like a calendar
 8 app or a fertility app, I would much more highly prize
 9 privacy and security in that case.
 10 And I do think that you have to present a
 11 holistic picture of these products and security --
 12 products and devices, which is what we're trying to do
 13 with the digital standard, but you can tell how hard it
 14 is because it's really -- not only do you have to
 15 effectively assess the privacy and security, and for our
 16 part, we can't assess what's happening on the back end;
 17 we can only look at the device itself. So we're -- even
 18 then, we're not even presented with a full picture of
 19 what the company is doing with your data.
 20 So I don't think it's failing. I just think that
 21 we're trying to catch up, and it's extremely hard,
 22 especially with the number of devices and products that
 23 are in the market. So we hope that we will be able to
 24 change the marketplace, you know, watch the space, and
 25 we'll be talking about some of our results in the coming

1 year, but just because it's hard for consumers and hard
 2 for intermediaries to do this kind of work doesn't mean
 3 that we don't have an interest in it.
 4 MR. WOOD: Okay, great.
 5 So let's step back a bit and ask a maybe related
 6 question. Is there a robust market for privacy products
 7 and services? Why or why not?
 8 MS. MCINNIS: So if I could just jump in on that,
 9 yesterday Citizen Lab out of the University of Toronto
 10 released a new security planner tool, which is a
 11 personalized experience for consumers to go through and
 12 answer questions based on not only their concerns with
 13 their online data but also the kinds of products that
 14 they use quite often.
 15 And then it presents them with a hierarchical
 16 list of what you can do to help protect yourself online
 17 and also gives an assessment of how much time and money
 18 it's going to take for you to implement these different
 19 choices. That just released yesterday. We already have
 20 over 5000 unique hits to the site, which is showing that
 21 people really do want these tools.
 22 It's just really hard, first of all, to
 23 effectuate the use -- the concerns and preferences
 24 across all of your devices, but also it's really hard to
 25 get a handle on your security online, and in some ways

1 it's good to just highlight a few areas, which they're
 2 doing on their security planner tool.
 3 Also, the number of individuals that the survey
 4 results pointed out doesn't necessarily mean action, but
 5 people are very, very concerned, and they have been
 6 pushing for better protections online. We saw the
 7 backlash after the Congress reversed the Broadband
 8 Privacy Rule under the Congressional Review Act. People
 9 really care about their privacy. They just feel like
 10 they don't have a way to effectuate these concerns
 11 effectively.
 12 MR. WOOD: Bob, did you have something to say?
 13 MR. GOURLEY: I do, I have a couple of comments.
 14 One, I agree, this is getting really hot, because, you
 15 know, all of us are buying all these devices with chips
 16 in it, you know, the internet of things. You know, the
 17 average home three years from now may have 600 devices
 18 in it that have chips that are communicating with your
 19 WIFI, with Bluetooth, with each other, by Zigbee, and
 20 these things have vulnerabilities, and we are going to
 21 need tools like this to understand how to protect our
 22 homes.
 23 There are commercial products available now that
 24 are aiming at the consumer in the home. The three
 25 biggest, as far as I know are, you know, Symantec has

1 something call the Core, Norton Core. Bitdefender has
 2 something you can put in your house, and then there's
 3 something provided by -- let's see, Norton, Bitdefender,
 4 and CUJO is another one. And what these things do is
 5 look at all of your internet of things devices and see
 6 what's normal.
 7 They report back, so you have to opt in to
 8 information sharing and you have to trust that company.
 9 You pay them a couple hundred dollars a year and they
 10 have a team of people watching your devices. How many
 11 people are going to pay for that couple hundred dollars
 12 a year? That remains to be seen.
 13 I would also say that -- Jennifer reminded me of
 14 something, and that is the analytic tools that are out
 15 there now may very well be a key threat to privacy.
 16 Right now we -- many of us have either the Android
 17 smartphones or Apple smartphones. If you get a call,
 18 sometimes it will say this call is possibly Tina,
 19 because of an email you received a year ago that had
 20 that phone number it. That's, in a way, creepy.
 21 That's not my contacts. They're going through my
 22 email and reading it through machine learning, or you
 23 start up your car and you look at your phone and it says
 24 it will take you 44 minutes to get home from here. How
 25 does it know I was going home? Well, because that's

1 what I usually do that time of day.
 2 Now, these are all examples of very discrete,
 3 little machine learning artificial intelligence
 4 solutions, but this stuff is growing now like it's on
 5 rocket fuel. If you look at Pinterest and what they can
 6 do now, if you pin an image, they now have machine
 7 learning tools that can look at that image and say
 8 that's -- not just that's a brown handbag, but here's
 9 exactly the type, and you may be interested in the
 10 following shoes. And did you know that when you were
 11 putting the image up there? And just watch this space
 12 of artificial intelligence and machine learning over the
 13 next three years, it really is on rocket fuel, and there
 14 are going to be privacy and security concerns that none
 15 of us have thought about.
 16 That also applies to, like, your medical data.
 17 There's going to be analytical tools that look over all
 18 your medical data, and all of a sudden you get called in
 19 for a meeting with the doctor you weren't expecting, and
 20 maybe that's good, maybe it's not. So there's so many
 21 of these issues that we just haven't thought through
 22 yet.
 23 MR. WOOD: Omri? I think Omri was first.
 24 MR. BEN-SHAHAR: Well, as Bob mentioned, there
 25 are options that are sold in the markets to enhance

1 one's sense of privacy and data protection, maybe also
 2 for security. I'm not an expert on that, but I have the
 3 strong sense that if there were demand, there would be
 4 supply.
 5 I recall that when the previous FCC was enacting
 6 its privacy rules, I looked at it, and I noticed that,
 7 you know, companies like Comcast and AT&T are offering
 8 no data collection packages, premium packages. It's
 9 just \$25 more per month, and yet, if I recall correctly,
 10 not many people were purchasing these options,
 11 suggesting that, you know, one of two things can happen.
 12 Maybe people really want it, but they don't
 13 understand, or people don't want it. I don't think that
 14 we can just proceed by saying -- and, you know, no
 15 matter what the evidence is, we'll say, oh, people just
 16 don't understand. If they did, they would want it. I
 17 think we have to consider what is this -- which of these
 18 two explanations is the right one, and that would have
 19 to be an empirical answer, do they understand or -- do
 20 they want it and don't understand or do they not want
 21 it?
 22 And one other quick observation is, in a study
 23 that was done, my colleague looked at the privacy
 24 practices of different websites, and they found that
 25 websites that deal with more sensitive issues have

1 heightened privacy practices. For example, adult sites
 2 don't share information; cloud computing sites have
 3 heightened security measures relative -- it's all
 4 relative, but there is some -- the only explanation for
 5 this is that there is some response to what these sites
 6 perceive to be priorities of consumers. So I would call
 7 that some form of a market response.
 8 MR. WOOD: Jennifer?
 9 MS. GLASGOW: Just real quick, I would like to
 10 differentiate privacy products that are directed to the
 11 consumer versus privacy products that are directed to
 12 the business. I'm a little skeptical that we're going
 13 to ever see really widespread adoption of the consumer
 14 products for all the reasons that we've been talking
 15 about, but I think the business community is very hungry
 16 for privacy-enhancing technologies and products that
 17 they can build into their products, because it may be
 18 far more tedious to develop the same kind of encryption
 19 or other type of activities that you would want to make
 20 more automated. So I encourage the development of
 21 commercially oriented privacy products.
 22 MR. WOOD: Okay, great.
 23 So I think we are going to move on to audience
 24 questions. The first one, which is maybe to the
 25 business folks -- but feel free to answer it, anybody --

1 is how do the panelists define or quantify reputational
 2 harm?
 3 MS. GLASGOW: Well, I'll jump in there. I think
 4 reputational harm is a harm that's evolving, and it's
 5 evolving at a pretty rapid rate. If you think about --
 6 it -- but it varies whether we're talking about harm to
 7 an individual or harm to a business entity, because
 8 reputational harm can come from both.
 9 We have had reputational harm in the business
 10 community from security breaches, although I'm sad to
 11 say -- and I don't have statistics to back this up, this
 12 is just my personal assessment -- that I think people
 13 are getting a little immune to security breaches,
 14 because there are so many of them, and, therefore, it is
 15 less of a differentiator from a company that has had one
 16 or hasn't.
 17 And I think that shows the consumer kind of has
 18 given up. They don't know what to do about it. They
 19 can't fix it, and even if they're -- as Bob described,
 20 if they're a victim, then they're not really sure
 21 whether there is anything to get panicked about or not.
 22 So I think that we've got a lot of work to do there.
 23 MR. WOOD: Anyone else? No? Okay.
 24 So the next question is, do all consumers suffer
 25 the same informational injury? For example, Professor

1 Ben-Shahar said that no rational consumer would want to
 2 be burdened with privacy and data security choices, but
 3 if consumers' desires are actually more diverse, might
 4 some consumers actually be injured by the deprivation of
 5 that choice, even if others were not?
 6 Do you want to --
 7 MR. BEN-SHAHAR: Sure. I want to correct the
 8 understanding of what I said or what I intended to say.
 9 No consumer -- many -- some consumers might want to be
 10 "burdened" with these choices. I think few, if any,
 11 would want to make choices on all aspects of the
 12 consumer transaction, and there are many, many of them,
 13 and there are many such transactions.
 14 It's just -- they're just not -- there's not
 15 enough time -- and people have studied it -- not enough
 16 time during the day to make these kind of choices
 17 affirmatively. Some things you need to let go and not
 18 make -- now, for some people, maybe the important things
 19 to choose are data privacy, and for others, it is -- it
 20 might be other aspects of the deal, maybe not so -- not
 21 necessarily that.
 22 I don't want to say about what the ratios are,
 23 because I haven't seen anything credible about that. I
 24 mean, people say that they want, but, you know, they
 25 don't behave as if they do. Any attempt to try to

1 simplify the entirety of the data privacy -- of the
 2 privacy policies into something like nutrition labels,
 3 to make people -- to make it possible for people to
 4 choose privacy like they choose food -- and to say in
 5 parentheses, I can't resist -- there is no evidence that
 6 nutrition labels changed people's diets in any
 7 meaningful way, but there is a strong perception that
 8 they do and that this is a model to choose.
 9 I tested that in my own work to try to create
 10 these kind of labels and to put people in a very nasty
 11 privacy setting, where they should really worry, to see
 12 whether they behaved differently when they are treated
 13 to these really friendly warning boxes as opposed to the
 14 very cluttered privacy policies, and unfortunately
 15 found, in a very large study, no effect. So it adds to
 16 my concern that people generally view these kinds of
 17 decisional aids as burdens.
 18 MR. WOOD: Okay.
 19 Katie?
 20 MS. MCINNIS: I would take Omri's burden and
 21 reclassify that as agency. A lot of consumers, as we've
 22 stated, don't feel like they have any control over their
 23 data, and some of the only ways that they can even try
 24 to effectuate their choices are through these opt-ins
 25 and opt-outs. And in some cases we have even seen, as

1 we saw in the recent Courts article, sometimes those
 2 preferences aren't even followed by the company.
 3 So consumers really desire these tools. This
 4 is -- yes, I think that the array of products that they
 5 interact with in daily life, that really does tire the
 6 consumer out to make all these decisions. I would agree
 7 with you on that, but I also think that this is one of
 8 the few ways that you can really try to have some agency
 9 over the data that you're sometimes sharing without your
 10 permission.
 11 And I would also emphasize that while, for many
 12 consumers, the privacy of what they're doing online or
 13 sharing with companies may not be a huge concern for
 14 them, members of commonly persecuted groups or outlier
 15 groups definitely have a huge interest in the privacy of
 16 their communications and actions online. Especially
 17 when we're looking at social organizers or protestors
 18 who are looking to effectuate change in the larger
 19 status quo, you definitely do have an interest in your
 20 privacy and your security online.
 21 I think if you didn't have that, we would see a
 22 huge chilling effect online. The NTIA did a study and
 23 found that since consumers feel so unsecured online,
 24 they have actually changed their practices online,
 25 right, and that's even before we got rid of -- before,

1 you know, net neutrality was taken away, before
 2 broadband privacy was taken away. So consumers are
 3 concerned. They just feel like there's a lack of
 4 control, and it's up to us and the regulators to provide
 5 more control for the agencies and the consumers, not
 6 less.
 7 MR. WOOD: Okay. I think we have time for one
 8 more question and then we'll leave a few minutes for
 9 last words from the panelists.
 10 How can industry and the FTC manage data mishaps?
 11 Audits? Who is the auditing agency? For reference, my
 12 teenager weighs risks daily, yet often makes decisions
 13 based on what she will get away with.
 14 Anybody want to take that?
 15 MS. MCINNIS: Unfortunately, the FTC has kind of
 16 a retroactive authority to act on these matters, except
 17 under a couple instances, such as COPPA. My personal
 18 dream is for the FTC to have more rulemaking power so
 19 that we don't have to act after the fact and after an
 20 injury has occurred in many cases.
 21 And I think that although we have a fragmented
 22 privacy regulatory environment in the U.S., as we have
 23 seen under COPPA and other regulations, we've also
 24 mentioned some of the constraints on financial
 25 transactions, I think that consumers really desire more

201

1 privacy and security over the data, and I wish that we
 2 had better -- although the FTC has had a great track
 3 record and I am not diminishing that, I think that we do
 4 look for better regulations and better protections at
 5 the federal level, especially since consumers have so
 6 few tools at hand.
 7 MR. WOOD: Okay.
 8 Anyone else?
 9 MS. HAN: Okay. Then let's move on to final
 10 thoughts. I will just go down the row, and you can take
 11 about a minute to give us any of your concluding
 12 remarks.
 13 Let's start with Omri.
 14 MR. BEN-SHAHAR: Well, I'll say one thing that,
 15 you know, the words that I've -- you know, the ideas
 16 that I shared today were largely skeptical about when --
 17 you know, what evidence do we have about injury. I
 18 don't want to sound like -- you know, to deny the
 19 possibility that good evidence will demonstrate that
 20 there is injury.
 21 I just want -- you know, I guess my main
 22 contribution, what I wanted to be a suggestion to the
 23 FTC, that to the extent that you identify something that
 24 needs to be done, that choice of regulatory technique is
 25 not transparency, informed consent, give consumers

202

1 control, improve the privacy policies, improve the
 2 format, give it in real time, real -- all of these
 3 things have been tried endlessly in so many other areas,
 4 including in privacy, and the performance of these tools
 5 is abysmal. They don't work. So if there is an injury
 6 to worry about, please, let's not worry about it through
 7 the tools of transparency.
 8 MS. HAN: Leigh?
 9 MS. FREUND: Yeah. Thank you again for having
 10 us. I think, you know, I would like to kind of focus us
 11 back on the purpose of the workshop here, which was
 12 trying to define what informational injury is and
 13 whether or not we can do anything about it, either at
 14 the FTC or in other places.
 15 I think, you know, we heard wildly different
 16 opinions from experts on what was an injury on the last
 17 panel, and I -- you know, and I want to really kind of
 18 focus on, you know, are we using data in a responsible
 19 way? Are we giving consumers power over their use of
 20 data? And how are we doing that in a way that mitigates
 21 both the risks and the benefits in that not only do
 22 businesses benefit, but consumers benefit.
 23 And I think, you know, kind of weighing those
 24 risk factors and the benefits and the risks together,
 25 you know, injury is a really big word, and it's very

203

1 difficult to quantify, but I think, you know, we have
 2 gotten some insights today into, you know, how serious
 3 something needs to be in order to call it injury, and
 4 the rest of it we put guardrails around to make sure
 5 that people are using data responsibly in our industry.
 6 MS. HAN: Thank you.
 7 Jennifer?
 8 MS. GLASGOW: I would kind of summarize by
 9 saying, first of all I think, when having these
 10 conversations, you have got to deal with security issues
 11 in one bucket and you have got to deal with appropriate
 12 use of information in another bucket. I like to think
 13 of the appropriate use of information as introducing
 14 ethics into that, and we have lots of models in various
 15 industry sectors.
 16 The legal sector -- many of you may be lawyers --
 17 are familiar with ethical approaches to things, and I
 18 think that there's a play there that we can begin to
 19 adopt when it comes to various uses of information as
 20 opposed to writing hard and fast rules about what you
 21 can and can't do. I agree with Leigh. Let's identify
 22 the really serious stuff and deal with it, and then --
 23 but there's a lot in the gray.
 24 The last thing I'll say is I think businesses are
 25 going to have to step up to doing more -- this ties not

204

1 just into the concept of security, but maybe, more
 2 importantly, into the concept of how they use
 3 information and/or how they share information and what
 4 they've done to satisfy the expectation of the consumer
 5 and what they've done to give choice to the consumer,
 6 because that is the entity that will make those calls in
 7 the end.
 8 And I think we're going to have to take some
 9 things off the table from the choice scenario. I don't
 10 want to have to give 50 choices when I buy my connected
 11 car because that's how many sensors are in the car. I
 12 want maybe three or four choices, and the rest of it, I
 13 want the car manufacturer to stand behind their decision
 14 to allow it or only use it in certain situations and so
 15 on.
 16 So I think we have to be cautious about giving
 17 consumers choices where there are varying differences in
 18 opinion and just helping them make the right choice when
 19 they're not.
 20 MS. HAN: Bob?
 21 MR. GOURLEY: Okay. So first I would say I'm
 22 with her, Jennifer, I really believe all that stuff.
 23 It's very important to consider both the security
 24 aspects and the inappropriate use and appropriate use of
 25 data aspects. It's very important. She's also the one

205

1 who first brought up the analytics and the future of
 2 analytics and that artificial intelligence is really
 3 going to be critically important.
 4 So many other things we didn't have time to
 5 discuss today, maybe it's going to be on the next panel,
 6 but things like tort law. Let's wait and see how these
 7 lawsuits around Equifax come out and are there other
 8 cases where companies should be sued because of
 9 negligence, and what will the courts do to shape the
 10 future of this dialogue, I think is a very important
 11 topic.
 12 Also, we didn't have time on this panel to really
 13 discuss best practices for businesses. There's so many
 14 of them out there that are captured and that need to be
 15 contextualized for businesses, but there are important
 16 best practices out there right now that more people need
 17 to know about.
 18 And the same for home, us people at home --
 19 Jennifer mentioned cars, of course, but cars, homes --
 20 all of your devices. What are best practices for those,
 21 we didn't have time to talk about. We did have time to
 22 talk about the big guys who are really managing our data
 23 and working hard to protect it, GAFA as I said, what
 24 would GAFA do, we need to keep looking at that. Those
 25 are my concluding thoughts.

206

1 MS. HAN: Thank you.
 2 Katie, you have the last word.
 3 MS. MCINNIS: Thank you for having us on this
 4 panel. I found it very interesting and it was also
 5 great to meet many of you in person.
 6 I just wanted to take a page out of Bob's book
 7 and mention that there's one thing that we didn't talk
 8 about, which is another injury to consumers, which is a
 9 loss of consumer power. If tons of information is being
 10 collected about me, with or without my knowledge, and
 11 that leads to first-party price discrimination, that is
 12 an injury to consumers, and that's one that I think
 13 we're overlooking and haven't paid enough attention to
 14 at this time.
 15 I also want to emphasize that Consumers Union and
 16 Consumer Reports, which is the same thing, is really
 17 looking to try and provide consumers with more agency
 18 and more ability in the marketplace really to decide
 19 what kind of products and services you want to use based
 20 not only on the services that these products provide but
 21 also based on the security and privacy of those
 22 services.
 23 And we hope that we can help change the
 24 marketplace so it is easier for consumers and so that we
 25 don't have to get tired out by all these different

207

1 disclosures, even though I personally see that more as
 2 an agency issue than a burden.
 3 And I wanted to point you all to the security
 4 planner from the University of Toronto's Citizen Lab
 5 which can help each and every one of you effectuate some
 6 privacy and data security protections while online. It
 7 can be tailored to you.
 8 Thank you, Cora and Dan, for organizing this
 9 panel.
 10 MS. HAN: Great. Thank you. So please join me
 11 in thanking our panelists.
 12 (Applause.)
 13 MS. HAN: It was a great discussion. We will be
 14 on break until 3:30, when our last panel on measuring
 15 injury will begin.
 16 (A brief recess was taken.)
 17
 18
 19
 20
 21
 22
 23
 24
 25

208

1 PANEL 4: MEASURING INJURY
 2 MR. SMITH: So, hi. Good afternoon. My name is
 3 Doug Smith, and my co-moderator on this panel is
 4 Jacqueline Connor. So welcome to the last panel of the
 5 day, measuring injury.
 6 As I think, you know, several times has been
 7 alluded to on the previous panels, there are particular
 8 empirical issues, or challenges that come up in trying
 9 to assess informational injury, and fortunately, today,
 10 we have a wonderful group of panelists to help us
 11 understand them.
 12 MS. CONNOR: Yes. As Doug said, we have five
 13 wonderful panelists with us this afternoon. So I am
 14 going to give you a brief introduction to each of them.
 15 First we have Garrett Glasgow, who is a senior
 16 consultant at NERA Economic Consulting, where he
 17 specializes in market competition, consumer protection,
 18 intellectual property, and environmental cases. He has
 19 presented and published on several topics related to
 20 damages stemming from violations of privacy or misuse of
 21 personally identifying information.
 22 Next to him we have Ginger Jin, who is a
 23 Professor of Economics at the University of Maryland,
 24 who was on leave at the FTC in 2015 to 2017, serving as
 25 Director of the FTC's Bureau of Economics from January

209

1 2016 to July 2017. Most of her research has focused on
 2 information asymmetry among economic agents and ways to
 3 overcome the information problem.
 4 Next we have Lynn Langton. She is the Chief of
 5 the Victimization Statistics Unit at the Bureau of
 6 Justice Statistics at the Department of Justice. She is
 7 responsible for overseeing the collection and the
 8 dissemination of data from the National Crime
 9 Victimization Survey, a large-scale survey of U.S.
 10 residents that serves as one of the two measures of
 11 crime in this country.
 12 Catherine Tucker is the Sloan Distinguished
 13 Professor of Management and Professor of Marketing at
 14 MIT's Sloan School of Management. Her research
 15 interests lie in how technology allows firms to use
 16 digital data to improve their operations and marketing,
 17 and then the challenges this poses for regulations
 18 designed to promote innovation.
 19 And last, but not least, we have Josephine Wolff,
 20 who is an Assistant Professor in the Public Policy and
 21 Computing Security Departments at the Rochester
 22 Institute of Technology. Her research interests include
 23 cyber security law and policy, the economics of
 24 information security, security metrics, incident
 25 reporting models, and insurance and liability protection

210

1 for computer security incidents.
 2 So first we would like to have each panelist talk
 3 a little bit about the work that they have done relating
 4 to measuring informational injury. So I'm going to read
 5 a brief question, and then if each of you could go down
 6 the line and kind of give a quick response to that, that
 7 would be great.
 8 So starting with Garrett and I guess working
 9 down, can you please give us a brief description of the
 10 research or work that you've done related to trying to
 11 measure injury in the context of privacy and data
 12 security issues?
 13 MR. GLASGOW: Yes. Thank you for having me here.
 14 In terms of privacy and misuse of personal data, I'm
 15 working in two areas. One -- which I call the easy
 16 area -- is misuse of information by companies, so where
 17 a customer and a company might have some kind of
 18 business relationship, certain levels of privacy or data
 19 protection are promised, and then the company for
 20 whatever reason doesn't live up to their promises.
 21 I've been working on, survey methods to try to
 22 value how much of the price the consumer pays for a
 23 product, bakes in this data protection or privacy.
 24 That's one area where I feel like we've made some good
 25 progress at NERA.

211

1 The other I call my blue sky research, and that's
 2 trying to determine whether there's an intrinsic value
 3 of privacy, so not the theft of data or the misuse of
 4 data, but do consumers, do individuals actually obtain
 5 some kind of utility or value from just knowing that
 6 their data is being kept private and is not being pried
 7 into by unauthorized people?
 8 This is an idea that comes from environmental
 9 economics, which is another area where I work, where we
 10 talk about the intrinsic value of the environment. It's
 11 not something that has value because it's the hub of a
 12 lot of economic activity, but it has what we call
 13 passive use value, where just we gain some kind of
 14 happiness or utility from just knowing that there's a
 15 pristine environment that hasn't been damaged, and if it
 16 is damaged, somebody's owed some kind of compensation.
 17 And so I've been doing research in that area as
 18 well to try to determine if privacy is similar to an
 19 ecosystem that might be damaged by bad acts or by
 20 carelessness.
 21 MS. CONNOR: Thank you.
 22 Ginger?
 23 MS. JIN: Thank you. Thank you so much for
 24 having me. I have to confess that I have done little
 25 research in this area before coming to FTC in 2016;

212

1 however, while I was at FTC, I dealt with a number of
 2 cases in privacy and data security which prompted me to
 3 think a lot about information injury.
 4 One crucial question is whether we should measure
 5 consumer harm in ex ante or ex post perspective. I know
 6 the second panel has already covered on this, but I
 7 still want to put in my two cents. The ex post
 8 perspective is quite intuitive. Somebody misuses
 9 consumer's information that results in say identity
 10 theft or a fraudulent transaction, and we can measure
 11 that by the amount of time, money, and effort that
 12 consumers lost because of this.
 13 However, the ex post perspective I would argue is
 14 narrow-minded because a lot of harm may not happen yet,
 15 but there's a risk there, or the harm has happened, but
 16 we cannot link to a particular firm who have done that
 17 data practice. So in these situations, we observe zero
 18 traceable harm, but that does not mean there is no
 19 consumer harm.
 20 I would also argue that, in fact, emphasis on ex
 21 post harm would end up encouraging overuse or misuse of
 22 data, because firms who engage in those misuse of data,
 23 they don't need to account for the negative externality
 24 they are imposing on the consumers. So in my view,
 25 that's inadequate.

213

1 In contrast, the ex ante perspective would
 2 emphasize the increase of risk to harm consumers even if
 3 that risk has not been realized or could not be traced
 4 back to a particular firm.
 5 So I heard a lot of panelists talking about
 6 Equifax. Myself is a victim of Equifax. I worry about
 7 my record on the black market. I end up paying
 8 something to try to freeze my account. I even sort of
 9 welcome the inconvenience, I have to lock and unlock on
 10 my account in order to get some credit in between.
 11 And to me, that's -- it spends my time and effort
 12 and money, and that is harm to me, even though that's --
 13 we haven't seen other harm coming back in my way, and
 14 it's probably very hard to trace that back.
 15 Similarly, if I know my favorite retailer has
 16 some bad data practice, even if that company has not had
 17 data breach, I will be worried. I would want to
 18 probably do something to reduce that risk. So in that
 19 sense, the ex ante perspective would say there is some
 20 harm there.
 21 And to follow on Garrett's suit, we can make an
 22 environmental analogy here. So, for example, a firm has
 23 polluted my neighborhood and exposed me to a higher risk
 24 of cancer. I would say the company should be
 25 responsible for that action even though I have not

214

1 developed cancer in my body yet, because it's increased
 2 the risk I'm exposed to. So in that sense, I believe
 3 the ex ante perspective is more appropriate.
 4 Another point I want to make is that the biggest
 5 difficulty in measuring harm is not measuring harm
 6 itself. It's measuring harm attributable to a specific
 7 firm. We can measure the extent of identity theft or
 8 other things, but exactly how to tie that back to a
 9 particular firm, I think that's the most difficult
 10 question.
 11 MS. CONNOR: Thank you, Ginger.
 12 Lynn?
 13 MS. LANGTON: Thank you for having me here today.
 14 As Jacqueline mentioned, I oversee the National Crime
 15 Victimization Survey, which is one of two measures of
 16 crime in the U.S. It dates back to the 1970s when it
 17 was developed to be a complement to police statistics
 18 because of the recognition that a large portion of crime
 19 goes unreported to police, and so if we just focus on
 20 those crimes that are reported to law enforcement, we're
 21 missing a big piece of the picture.
 22 And this is particularly true when you're talking
 23 about sensitive crimes and when you're talking about
 24 more of what we would call sort of white collar crimes
 25 or emerging crimes -- though I don't think "emerging" is

215

1 really the correct term anymore -- so crimes like
 2 identity theft and fraud that are highly unreported to
 3 police. So the NCVS is a household-based survey. It's
 4 conducted for BJS by the U.S. Census Bureau.
 5 We go to an incredibly large sample of households
 6 and interview all persons age 12 and older within those
 7 households about their experiences with victimizations.
 8 So our sample size is -- right now we go to over 200,000
 9 people every year, and we get response rates in the high
 10 seventies. So if you do survey research at all, you
 11 know that that's pretty remarkable at this point in
 12 time, still -- and we ask questions about their
 13 experiences with victimization and also the nature of
 14 that victimization and the victim response to that
 15 victimization. So as Ginger was just speaking about,
 16 this is the ex post perspective very much.
 17 The National Crime Victimization Survey focuses
 18 specifically on violent and property crime, but we do
 19 conduct a number of supplements to the survey, and the
 20 one that I think is most relevant for the conversation
 21 today is a supplement that we have been conducting for a
 22 number of years on identity theft.
 23 Of course, identity theft is just one type of
 24 informational injury. Again, ex post, very specific
 25 harms associated perhaps with a data breach and often

216

1 just because of misuse of personal information through
 2 other means, but I think there are some important things
 3 that we can glean from the identity theft supplement
 4 that are relevant to the broader conversation here
 5 today.
 6 So the supplement collects information about the
 7 attributes of victims and victimizations and the
 8 response to victimization, but it also asks questions
 9 about the harms experienced by victims who suffered from
 10 identity theft, and on top of that, it asks victims and
 11 nonvictims about behaviors that they engaged in to
 12 prevent any type of misuse of their identifying
 13 information and also whether they have experienced any
 14 kind of data breach in the past 12 months.
 15 So when we look at that information, we can see
 16 that among individuals who have experienced a data
 17 breach, the risk of identity theft or the prevalence of
 18 identity theft is double that of those that have not
 19 experienced a breach -- not that surprising, but putting
 20 numbers behind what we know to be true or assume to be
 21 true. And then among identity theft victims, about 20
 22 percent of the victims in our survey say they also
 23 experienced a data breach during that reference period.
 24 So there's certainly a correlation there, not
 25 surprising.

217

1 I think the other point that's important to take
 2 away, though, is that even among identity theft victims
 3 that experience no financial losses -- so they have no
 4 financial losses whatsoever -- there are still harms.
 5 So we asked them questions about not just their losses
 6 and the time spent, but also about how distressing they
 7 thought that the incident was, and even among those
 8 identity theft victims that didn't experience financial
 9 loss, about 30 percent still found the incident to be
 10 moderately to severely distressing. So that suggests
 11 that, in and of itself, the experience of having your
 12 information misused, having your information out there,
 13 has some harm to victims, and so I think that's relevant
 14 for our conversation today.

15 MS. TUCKER: All right. So I'm Catherine Tucker,
 16 and I am an empirical economist, which means that I'm
 17 going to behave in a predictably economist way and say
 18 two things.

19 The first thing is a lot of my research has been
 20 focused on how hard it is to actually measure this, and,
 21 in particular, my research, which is focused on the use
 22 of algorithms and AI, suggests this is just going to get
 23 harder and harder as the boundaries of an individual's
 24 data gets fuzzier and fuzzier.

25 The second thing which I'm going to say, which is

218

1 predictably economist, is that my research is really
 2 focused a lot on documenting the trade-offs which come
 3 from trying to protect consumers and their privacy, and
 4 let me tell you a little -- give you sort of three
 5 typical unintended consequences that I've found in that
 6 research.

7 So the first unintended consequence I want to
 8 highlight is often when we have privacy or data breach
 9 regulations, we're very focused on the idea of big
 10 companies and the idea that they need to be provoked to
 11 do something better, but my research suggests that it's
 12 actually smaller companies, startups, which tend to be
 13 most adversely affected in terms of the costs of this
 14 kind of regulation.

15 The next piece of research of unintended
 16 consequences I want to highlight is some research I did
 17 into data breach notification laws and, in particular,
 18 what happened when they gave exceptions to encryption.
 19 Now, in this research, what we found is that actually
 20 there were more data breaches as a result of these
 21 exemptions. And why was that? Well, they just focused
 22 on encryption, and it meant you had a whole lot more
 23 doctors losing laptops from their car as a result of
 24 people focusing on just one dimension of data security.

25 Now, the last thing I just want to highlight as

219

1 an unintended consequence is some research we've
 2 recently done about patient data and hospitals which
 3 highlights that actually hospitals are using data
 4 security and privacy regulations to actually stop
 5 patients themselves getting access to their medical data
 6 records they need if they try and transfer hospitals.
 7 And you -- some people in the room, I see you nodding,
 8 right? You have experienced this in trying to get your
 9 own medical data out of the system.

10 MS. WOLFF: Thank you.

11 So I've worked on a couple of areas related to
 12 thinking about the injury and the types of harm that
 13 come out of data breaches and cyber security incidents
 14 more generally, and the first time I sort of encountered
 15 this was in a project looking at the aftermath of
 16 security incidents and trying to trace who ends up suing
 17 whom and who ends up paying whom, and a lot of this is
 18 at the corporate level.

19 A lot of this is the credit card companies and
 20 payment networks suing breached retailers and demanding
 21 certain amounts to settle the fraud costs, and then
 22 there are also a number of the consumer class action
 23 suits that you heard talked about a little bit on the
 24 panel before lunch, and for all the reasons that they
 25 brought up on that panel, those are often very hard, to

220

1 see sort of go through or even get heard by courts, and
 2 I got interested in this question of sort of how sort of
 3 different types of policy agencies, different parts of
 4 the government, and different parts of industry think
 5 about and understand these types of harms or injuries.

6 And so I did another project looking across sort
 7 of the different ways that people had tried to measure
 8 them and bucketing a couple different kinds of data.
 9 There's a lot of survey data in this space, a lot of,
 10 you know, sending out reports to different companies and
 11 saying, how much did you lose due to breaches in the
 12 last year, and putting that together as sort of
 13 self-reported data to think about how much we think
 14 these breaches cost to the companies, to their customers
 15 sometimes.

16 One of the big sources that some of you may have
 17 seen is the Ponemon study that comes out every year,
 18 again, focused on self-reported numbers and trying to
 19 stack those up against some of the other data sources
 20 that we sometimes use to think about quantifying these
 21 types of harm. One of those was insurance claims.
 22 NetDiligence has a data set of companies that have filed
 23 cyber insurance claims for harms due to computer-related
 24 losses and looking at sort of how the numbers change if
 25 you look at what they file for insurance versus what

221

1 they report in a survey about these losses.
 2 And then, finally, looking at a lot of the
 3 analysis that's been done around stock prices and market
 4 value of breach companies and trying to understand sort
 5 of how that tells a slightly different story if you use
 6 that as a proxy for thinking about the costs or the
 7 consequences of breaches.
 8 And then to come back to sort of thinking about
 9 the consumer injury and not just the losses to a
 10 company, but also to individuals. I spend a lot of time
 11 looking at the firms that are offering cyber insurance
 12 policies now and how they price those and how they think
 13 about the kinds of harm or losses that they will or
 14 won't cover, and increasingly, we're seeing a lot of
 15 them get into the still relatively small market of
 16 personal cyber insurance, selling policies to you
 17 individually or to your family to cover certain kinds of
 18 losses and trying to understand how it is that we
 19 understand the ways people are purchasing those types of
 20 policies, what kinds of things we're covering with them,
 21 as a way of thinking about the types of losses that
 22 people are concerned about.
 23 And also, coming back to sort of some of the
 24 skepticism you heard on the previous panel from Omri
 25 about, you know, what do people actually do, not what do

222

1 they say they care about, but what are they actually
 2 willing to pay for? What can we see, when we look at
 3 this emerging personal cyber insurance market, about the
 4 types of injury customers seem most concerned about and
 5 are most willing to actually pay for protection?
 6 MR. SMITH: All right. Thank you, guys.
 7 So now we will sort of jump into the discussion.
 8 We are going to start off, I think, by talking about
 9 kind of trying to measure preferences, right, trying to
 10 understand what consumers value. And so I think a good
 11 place to start that would be sort of how to measure --
 12 just what consumers say about what they value. And,
 13 Garrett, you talked about doing surveys on this, so
 14 maybe if you could tell us a little bit about how that
 15 works.
 16 MR. GLASGOW: Sure. So, yeah, my work in
 17 measuring privacy, measuring the value of data, has
 18 primarily been survey-based. Before coming to NERA
 19 about 3 1/2 years ago, I was a professor in the
 20 Political Science Department at UC Santa Barbara, where
 21 I did lots of survey research, so maybe it was natural
 22 that I fell into a survey-based approach to looking at
 23 privacy and the value of data, and there are two
 24 different approaches that I've looked at.
 25 There's what's known as conjoint analysis, and

223

1 then there's contingent valuation, two different survey
 2 type approaches, and I'll just briefly talk about each
 3 and then the strengths and weaknesses of each of these
 4 approaches.
 5 Conjoint analysis is well known in consumer
 6 research. It's accepted in court as a reliable method
 7 for uncovering truth in a lot of contexts. And what
 8 conjoint analysis involves is we ask our survey
 9 respondents to make choices, as if they were in the
 10 market making choices, from among some set of
 11 hypothetical products, and these products are going to
 12 have different features or attributes, and so we can
 13 see, if they make enough choices, which attributes they
 14 seem to value and which ones are unimportant.
 15 I'll give you an example from my own research.
 16 We did research on streaming video services, and we
 17 present people with, say, pretend you're in the market
 18 to update your streaming video service. Here are some
 19 services that might be available to you. They might
 20 have different streaming speeds; some might have
 21 high-definition available; some might have more
 22 television shows; of course, different monthly prices
 23 and so on.
 24 We just present these different services and say,
 25 well, pretend these are the three that are available in

224

1 your area or that you could possibly purchase. Which
 2 one of these services would you purchase? And they can
 3 make those choices.
 4 Now, when we want to bring this to privacy, one
 5 way we can do this is just regard privacy as just
 6 another feature of a product. Obviously, this is only
 7 going to work if we're looking at a situation where it's
 8 a consumer engaging in a market transaction with some
 9 company that's made some kind of promise about privacy
 10 or how they are going to treat your data.
 11 So we can say, what we did with this paper that
 12 I'm talking about, is part of that streaming video
 13 service was, and then there's different possible privacy
 14 policies that these services offer. They might say that
 15 we never share your data. Others might say, well, we'll
 16 collect your viewing habits, not your personal
 17 information, but we will collect your viewing habits and
 18 package those up and use those to help content providers
 19 decide what kinds of shows to make. And then the third
 20 option is maybe we collect your personal information as
 21 well, and we might share that with third-party
 22 marketers, and so on.
 23 And what we were able to do with this survey was
 24 see what value do people place on protecting their data,
 25 or conversely, what kind of discount do we need to offer

225

1 consumers to get them to agree to share different types
 2 of data?
 3 The strengths are this is a really
 4 straightforward, reliable way to measure consumer
 5 preferences. It's widely used. It's widely understood.
 6 I regard its main weakness as narrowness. As I said,
 7 these are consumers engaged in a market transaction.
 8 What do we do in all the privacy cases where there isn't
 9 a market transaction, like a data breach?
 10 I mean, I suppose we could design some kind of
 11 conjoint analysis where we say, now pretend there's a
 12 certain percent chance that this company is going to
 13 have a data breach in the next year, but I don't think
 14 most consumers think about their purchases that way.
 15 It's a strange hypothetical to pose to people, and I
 16 think you would get really strange results with a survey
 17 like that. Maybe it's possible to do, but I think
 18 that's one of the main weaknesses.
 19 But at least in areas where we can apply this,
 20 this conjoint analysis lets us measure the value that
 21 individuals are placing on their privacy or on different
 22 data-sharing policies, gives us what we call a
 23 willingness to pay to protect their data, and then we're
 24 talking about quantifying damages. If a company doesn't
 25 live up to that promise, we can use that willingness to

226

1 pay to calculate damages, that we can use that as a
 2 basis to say a certain percentage of this price was
 3 privacy protection, you didn't live up to privacy
 4 protection, you owe consumers some refund or some amount
 5 of damages based on your failure to live up to your
 6 promise.
 7 I mentioned earlier, there's easy cases and hard
 8 cases. I think those are kind of the easy cases. I
 9 think we have made some headway in terms of measuring
 10 the value of information, the value of privacy there.
 11 Hard cases are all the other ones, things like
 12 data breaches and so on, and one possible approach to
 13 that is what's known as contingent valuation, and to
 14 really -- you know, a really rough description of that
 15 would be, well, asking people how much compensation they
 16 would need if some bad event happened. This is very
 17 common in the environmental setting, in areas where
 18 there isn't a market transaction. There isn't a market
 19 for the environment, but there could still be damage
 20 done, and there might still be compensation owed.
 21 The classic example of contingent valuation came
 22 from the Exxon Valdez spill. So the Exxon Valdez was a
 23 big tanker that spilled a whole bunch of oil in Prince
 24 William Sound up in Alaska. It's a place most people
 25 have never seen. There is not really much economic

227

1 activity going on there except for the tankers going
 2 through, but people still felt aggrieved, they were
 3 still damaged.
 4 How do we measure what kind of compensation Exxon
 5 might owe to the American people? And one way that this
 6 could be done would be contingent valuation. They went
 7 out and conducted surveys. They said, well, suppose we
 8 had to increase taxes next to year to create a system,
 9 maybe a tugboat system, that would make sure these kinds
 10 of spills didn't happen again? How much would you pay
 11 to prevent this from happening?
 12 And people would give us answers, and you could
 13 tabulate that up and say that this is the value of that
 14 environment to these people. You can easily see taking
 15 this over to a data breach environment or a privacy
 16 environment, where we say a data breach has happened.
 17 How much would you pay to do business with a company
 18 that has some lock-down system where they have reduced
 19 the chance of a data breach to almost nothing? We can
 20 see designing a survey that would be something along
 21 these lines.
 22 The strengths here are that this is -- unlike
 23 some other surveys, this is something we can at least
 24 apply to something that's not a traditional market
 25 transaction. A data breach is not a traditional market

228

1 transaction. The weaknesses are that these are kind of
 2 strange hypotheticals that we're presenting to people.
 3 It's -- and people -- especially with issues that are a
 4 bit emotional, things like environmental damage or
 5 privacy or data breaches, people often give what are
 6 known as socially desirable or protest answers.
 7 How much would you pay to clean up Prince William
 8 Sound? We will have people say, I'd pay \$50,000 to
 9 clean up Prince William Sound. Well, their income was
 10 \$45,000. They are just trying to signal to us that
 11 they're angry about what's happened. And I would
 12 imagine with doing surveys on data breaches, you would
 13 get the same kind of anger and the same kind of protest
 14 answers, where people want to signal that they are angry
 15 at companies for allowing a data breach to happen or for
 16 leaking their data, and it might not be very useful in
 17 terms of measuring damages, but that is one possible
 18 survey approach to dealing with data breaches. I'll
 19 talk more about that later on, but those are the --
 20 that's an overview of two major survey approaches.
 21 MR. SMITH: Great. I want to open this question
 22 up to all of the panelists, but first, I know, Catherine
 23 Tucker, you have done some work in this area, so I was
 24 wondering if you could sort of comment on what you have
 25 done and found.

1 MS. TUCKER: Oh, yes. So just as I previewed, it
2 is going to be about the difficulties in this, and the
3 work I did was basically investigating something we call
4 the privacy paradox, which is that if you ask people in
5 a survey how much they care about privacy, everyone
6 cares about it, but then we see all this actual behavior
7 which is inconsistent with that stated preference.

8 Now, what we did in this study is we -- it took
9 place among the MIT undergraduate population, and we
10 asked them to take part in a study, and as a reward,
11 they got \$100 in Bitcoin, and this was in 2014, so those
12 of you who can do the math, this is a lot of money right
13 now. We made a good call, that.

14 So when we did this study, one of the questions
15 we asked them for was some data on some really quite
16 personal and sensitive information, which was data about
17 their friends' contact details. Now, in the ordinary
18 setting, when we asked this question, a surprising
19 number of our MIT undergraduates really decided they
20 were not going to answer this question, but instead,
21 they were going to give us fake information, and we knew
22 it was fake because of their use of swear words and
23 their use -- and the use of swear words employed to
24 describe what they thought about us for actually asking
25 this question as part of the email. So it was

1 MS. JIN: Yeah. I just want to follow up with
2 Catherine's comments on the privacy paradox and how
3 actions seem to differ a lot from stated preferences. I
4 think the biggest question is to distinguish different
5 explanations behind this. Is this because consumers
6 don't know the risks that they are willing to give away,
7 or because they know the risks but they somehow believe
8 the benefits dominates the risk, or they see the extra
9 risk of giving away this to one more person, given that
10 their data probably has already been breached multiple
11 times, is so small that they feel helpless, and so,
12 therefore, they give away?

13 I think those explanations would sort of imply
14 very different policy actions. It would be -- I will be
15 really interested to see if future research will be able
16 to distinguish those explanations.

17 MR. SMITH: Thanks, Ginger.
18 Lynn?

19 MS. LANGTON: So as I'm sitting here thinking
20 about measuring actions, I'm realizing that there is
21 more that we could potentially be doing with our survey.
22 So we're not getting at consumer preferences in any way,
23 but we are asking a series of questions about behaviors
24 that they engaged to -- again, this is in the context of
25 identity theft -- but behaviors they engaged to

1 definitely deliberate. Now, that was the first setting.

2 And then for half of them, we changed the context
3 somewhat in that we gave them an offer of cheese pizza,
4 and if you're wondering how much cheese pizza, sort of a
5 slice of cheese pizza. And what we found was that when
6 there was no cheese pizza involved, people tend to
7 behave in a way which was consistent with what they said
8 in a survey about their privacy preferences, but the
9 moment we gave them the offer of cheese pizza, even
10 those people who said they really care deeply about
11 privacy started giving away this quite sensitive data.

12 Now, you know, in terms of interpreting it, it's
13 really quite hard, right? One thing you could do is
14 sort of a typical economist response, which is that
15 stated preferences, it's hard to use them to measure
16 anything, and we should use revealed preferences.
17 Another interpretation of the study is, though, oh, my
18 gosh, if MIT undergraduates behave like this, people who
19 should really understand technology, maybe we need to
20 really protect people to actually get them to behave in
21 line with their stated preferences. So no conclusions,
22 just some difficulties in terms of using survey
23 responses.

24 MR. SMITH: Thank you, Catherine.
25 Ginger, do you have any thoughts about --

1 prevent the misuse of their personal information, and I
2 think, again, this speaks to what they're actually
3 doing.

4 So, you know, these are pretty basic things, but
5 I think the proportion of people that do these things
6 regularly is still pretty surprising. So if you ask
7 them if they check their bank and credit statements,
8 okay, 76 percent say they do that, which makes me wonder
9 about the other quarter of people, I have to say. Who
10 doesn't ever check their bank statement? But that's a
11 different subject.

12 But then when you -- you know, when you move into
13 things like do people regularly change passwords on
14 financial accounts, about 30 percent say they do;
15 checked their credit reports, that's about 40 percent;
16 purchased identity theft insurance or a credit
17 monitoring service, again, maybe this gets more into
18 that willingness to actually pay, to spend money on
19 something that might prevent this from happening, and
20 that's only 5 percent of the residents that are
21 participating in the survey that say they actively do
22 this.

23 So now I'm thinking, what could we ask? Could we
24 ask some questions related to data breaches specifically
25 that would get at their -- the behaviors that they

1 engage in? So even just how often do you consider
2 whether a company has had any sort of breach that you
3 can find information about before you provide your
4 information to them, just to kind of gauge whether or
5 not there are actions being taken to actively avoid
6 potential situations.

7 And, again, that -- companies can change over
8 time, and so that would -- you know, those are
9 challenging things to measure, but I think there are
10 still some actions that we could think about concretely
11 getting at that would address this issue a little bit
12 more.

13 MR. SMITH: Thanks, Lynn. And I think, you know,
14 talking about that, you sort of broadened the
15 conversation to looking directly at people's actions or
16 at least their purported actions.

17 So, Josephine, would you like to comment on
18 either sort of stated preferences or revealed
19 preferences or both?

20 MS. WOLFF: Sure. Well I think, you know, a lot
21 of what we have when we look at the data people have
22 analyzed and collected around the injuries and costs
23 associated with data breaches is very much stated
24 preferences. Most of what you see, especially, say, in
25 industry reports, is going to be kind of self-reporting,

1 this is how much this breach cost, or this is how I was
2 affected, these were the injuries.

3 And so I think that we start out from a position
4 of basing a lot of our estimates, basing a lot of our
5 understanding of these types of costs on those stated
6 preferences just for practical reasons, that that was
7 sort of the -- and still is in a lot of ways -- the data
8 that's easiest to collect in large volume, and it's
9 definitely true, and several of the other panelists have
10 brought it up, there's a huge discrepancy when you start
11 trying to compare that to what people are actually
12 doing.

13 It's very hard, as Ginger says, to get at why
14 exactly that is, and I think one of the things that's
15 complicated when I, say, look at legal cases around
16 these class action suits and the aftermath of data
17 breaches, is that getting involved in one of those class
18 action suits is not always just a sort of
19 straightforward question, do I care about my data? Do I
20 value my privacy to some amount of time?

21 And the strongest example of this I think is
22 probably the Ashley Madison class action lawsuit, where
23 the judge actually decided if you want to go forward as
24 a member of this class action lawsuit, you are going to
25 have to use your real name, right? So it was this sort

1 of complicated decision for everybody whose data had
2 been stored by Ashley Madison and breached, that, okay,
3 on the one hand, I valued that data and the loss of
4 privacy that came, with everybody in the whole world
5 potentially knowing that I'm a member of this website
6 for adulterous affairs, but on the other hand, if I now
7 move forward with trying to pursue that as an injury in
8 court, I am going to lose this privacy in a slightly
9 different way.

10 That kind of decision, I think, is not actually
11 as straightforward as saying, oh, I guess nobody cares
12 about the injury that was done to them in this data
13 breach because they are not willing to pursue this
14 lawsuit, but more about trying to understand what are
15 the actual decisions that people are making when it
16 comes down to acting on what they think are their
17 preferences, on what they think is what they value.

18 MR. SMITH: So in some sense understanding sort
19 of the costs of the trade-off, the benefits of privacy,
20 it's sort of important to figure out how to measure it?

21 MS. WOLFF: Absolutely, and I think it gets at
22 some of that discrepancy we see, which would be sort of
23 how much I think I value my privacy and the things I'm
24 actually maybe willing to do in practice to protect it
25 or pursue my losses.

1 MR. SMITH: Okay, thanks, Josephine
2 So do people have any further thoughts about sort
3 of measuring consumer preferences through their actions?
4 MR. GLASGOW: Yeah. Actually, I think we have
5 had heard several different stories now about a mismatch
6 between a consumer's stated preferences and consumer
7 actions, and this is a regular feature of privacy
8 research. We see this a lot, that people seem to take
9 actions that contradict what they have stated matters to
10 them. And I think that it's often used to dismiss the
11 concerns of consumers in what I think is an unfair way.

12 It's a complicated issue, whether you -- people
13 might be willing to take some actions in some contexts
14 but not in others. I'll give you one example from my
15 research, that conjoint analysis I mentioned on
16 streaming video services. About 10 percent of our
17 survey respondents said I would never choose a streaming
18 video service that collects any information about me,
19 whether that be movies about -- which movies I watch or
20 personal information or anything like that, but one of
21 our screening questions to get into our survey was, do
22 you have currently have a streaming video service?
23 People had to say yes to get into the survey.

24 So 10 percent of people already had a streaming
25 video service that was collecting information about

1 them. I don't know how many of you saw the Netflix
 2 tweet from yesterday or the day before, but Netflix sent
 3 out a tweet that said for the 57 of you that have
 4 watched The Christmas Prince 18 times in a row, are you
 5 guys okay? It was something like that. So they clearly
 6 are collecting information on who's watching what, and
 7 they even sent out a tweet kind of teasing people about
 8 movie choices.

9 So what's happening with this 10 percent of
 10 people in the survey that said I would never choose a
 11 streaming video service that shares my information, yet
 12 they already are doing business with one? One
 13 possibility is just lack of information. They weren't
 14 actually aware that the streaming video services are
 15 collecting this information, and that's one possibility
 16 for this mismatch between action and preference,
 17 although if somebody is really a privacy hawk and says I
 18 would never share information, they probably know who's
 19 sharing what.

20 Another possibility is -- this is that signaling
 21 of importance that I mentioned earlier, where you give a
 22 protest answer. So maybe those 10 percent of people,
 23 even though we tried to be careful, they figured out
 24 this isn't a survey about streaming video services.
 25 This is a survey about privacy, so I am going to send a

1 signal that I value privacy by saying I never share
 2 anything, and that will let those researchers know that
 3 this is really important to me. That's another
 4 possibility for the mismatch. It's not that the
 5 consumers are being inconsistent, just that we failed as
 6 researchers to try to hide what we were trying to get at
 7 and honestly measure that.

8 Then the third possibility is the context. In
 9 some situations, you're willing to share, and in some
 10 situations you're not, and consumers would like to pick
 11 and choose, or in some cases you might perceive a threat
 12 and in other cases you might not.

13 And I'll end with another little story. This is
 14 from about three years ago. An artist baked some really
 15 fancy cookies that had the Facebook logo and the Google
 16 logo and so on and went out into New York City and gave
 17 them away to people -- well, didn't give them away --
 18 didn't sell them, but they said you have to give me
 19 personal information if you want this cookie.

20 And about half of the people were willing to let
 21 their photograph be taken in exchange for a cookie.
 22 Half of the people were willing to give what they said
 23 were the last four digits of their Social Security
 24 number. They -- a lot of these people were willing to
 25 let her write down information off their driver's

1 license in order to get a cookie. And one-third of
 2 people were willing to give up their fingerprints for a
 3 cookie.

4 So you say, well, how do we reconcile that with
 5 people who say they care about privacy? Well, maybe
 6 there's a context issue here, that an art student
 7 probably isn't going to take those fingerprints and then
 8 go rob a bank using them or something like that. There
 9 is probably a very low risk there, but if a data hacker
 10 gets the same kind of information and it winds up on the
 11 black market, that's a very different risk.

12 So I don't have answers to this necessarily, but
 13 I would say there's often a mismatch between preferences
 14 and actions when it comes to privacy. It doesn't
 15 necessarily mean that consumers don't know what they're
 16 doing. It's a complicated issue.

17 MR. SMITH: Thanks.

18 Ginger, do you have any further thoughts?

19 MS. JIN: Yeah. I just want to emphasize that,
 20 as an economist, I often believe actions are louder than
 21 words, but in this particular area, I really believe the
 22 survey approach and the revealed preference approach
 23 should be really complements to each other. We actually
 24 have already seen some interactions here while Catherine
 25 has been talking about sort of MIT student action in the

1 lab, while Lynn was trying to think about how you can
 2 design a better survey question to get at that sort of
 3 behavior in a national representative sample.

4 I guess the feedback could go the other way, that
 5 if we know, for example, consumer lack of information or
 6 feeling helpless is one of the primary reasons for them
 7 to behave a certain way, maybe Catherine can design a
 8 very clever lab experiment to determine or to really
 9 tease out people's actions. I really see the positive
 10 complementarity between the two approaches.

11 MR. SMITH: So we're kind of going long on this
 12 topic, but, Lynn, do you have any sort of last thoughts
 13 on this?

14 MS. LANGTON: I'm sorry?

15 MR. SMITH: Do you have any last thoughts on this
 16 before we move on to outcomes?

17 MS. TUCKER: Yeah. I would just like to also
 18 add, to make it worse, that actions don't always
 19 translate to actions in the way we would like, and if
 20 you sort of move along in the Bitcoin study I was
 21 talking about, we then tested really how much laziness
 22 affects people's privacy preferences, in that we asked
 23 them what wallet they wanted them to put their Bitcoin
 24 in. We gave them a variety of wallets, some of which
 25 protected their privacy, some of which completely

1 didn't, and the biggest predictor of what wallet they
 2 chose was not their privacy practices. It was, instead,
 3 how far up on the page that wallet was.
 4 Then, we then said, okay, well, maybe it's just
 5 like a lack of information, so half of the students saw
 6 lots of information about the wallets, basically
 7 everything you could ever want to know, and there was
 8 some good news in that that reduced, shall we say, half
 9 of the laziness, but I guess the bad news is there was
 10 still half of the laziness there even for people
 11 expressing a lot of privacy preferences.
 12 So in other ways, you can actually change
 13 people's actions a lot simply by the context in which
 14 you get them to make the choices, making even this
 15 action data hard to judge, I'm afraid.
 16 MR. SMITH: Josephine, any last thoughts on --
 17 MS. WOLFF: Well, I think -- I mean, I think what
 18 Ginger says about needing both the survey and the
 19 revealed preference data is really important because I
 20 think there are certain types of injuries, and you heard
 21 a lot about that this morning, all the different ways
 22 that people can be affected by data breaches.
 23 I think there are some of those injuries that we
 24 really have no other way to get at, especially when
 25 we're talking after a breach has occurred, when we are

1 not necessarily going to say that all of the different
 2 types of emotional or psychological harm you may have
 3 suffered are things you can obviously mitigate, right?
 4 It's one thing to say, well, people didn't go and
 5 change their passwords or people didn't go and file a
 6 class action lawsuit, but if all of your emails have
 7 been released in the Sony breach, then it's not obvious
 8 what the action you would take would be to demonstrate
 9 that that really affected you, that that was a real kind
 10 of injury.
 11 So I certainly think it's true that the
 12 self-reported data has a role to play in this. I think
 13 where it becomes tricky is when you're looking at really
 14 kind of crisp quantification for things like legal
 15 remedies or policy interventions, whether there's any
 16 way to turn that into something that can be calculated
 17 precisely enough for those types of remedies.
 18 MR. SMITH: Okay, thanks, Josphine.
 19 So we are going to have to leave the topic of
 20 preferences and move on to, you know, an alternative,
 21 which is to just straight up measure outcomes and try to
 22 understand things that way.
 23 So, Lynn, I'd like to hear more about sort of how
 24 your study allows us to get at that question.
 25 MS. LANGTON: So, again, we're talking in the

1 context of identity theft here, so beyond just any sort
 2 of data breach or privacy-related issue, but we ask a
 3 whole series of questions related to both tangible and
 4 intangible harms -- again, ex post harms -- associated
 5 with the misuse of personal information.
 6 So, of course, we ask about financial losses;
 7 that's an obvious one that you have to include. We also
 8 ask about the amount of time that an individual had to
 9 spend clearing up the issues related to the
 10 victimization. And then we ask a whole series of other
 11 questions trying to get more at some of these
 12 intangibles.
 13 So I mentioned already that we ask about
 14 distress. We also asked about whether the incident
 15 resulted in any problems with family, friends, work,
 16 school. And then we asked questions about whether they
 17 experienced any credit problems related to the incident;
 18 whether they experienced any legal problems related to
 19 the incident; whether they had to deal with debt
 20 collectors. So these are some of those more
 21 intangibles.
 22 And then, you know, I think to get more at those
 23 intangibles, too, and, like, really the impact of an
 24 incident on an individual -- and, again, this goes
 25 broader than identity theft -- you know, the other thing

1 that we can do is then sort of cross these different
 2 types of outcomes and different types of harm.
 3 So when we look at, for example, how much time an
 4 individual has to spend dealing with an issue, and then
 5 we look at the level of distress, I mean, there's a
 6 positive linear relationship there that's pretty strong.
 7 So when an individual has to spend six months or more
 8 dealing with this misuse of their information, you know,
 9 a large portion of them say they were severely
 10 distressed, whereas if they're able to resolve it in a
 11 day or so, you know, a smaller portion say that it was
 12 severely distressing.
 13 So, again, it's indirectly translatable to data
 14 breaches, but I think sort of the same ideas, and you
 15 can use survey research to sort of tap into these ex
 16 post responses and harms that victims experience as a
 17 result of these incidents.
 18 MR. SMITH: Thanks, Lynn.
 19 Catherine, do you have any thoughts about this,
 20 about sort of measuring outcomes, what data we might
 21 look for or how we might take things that are sort of
 22 less tangible and convert them into something we can
 23 sort of quantify?
 24 MS. TUCKER: Well, so, my thought actually was
 25 that really when it comes to measuring injury, I think

245

1 we lack a good model of the supply side of people who
 2 want to do injury. And what do I mean by that?
 3 Well, I've seen some really intriguing research
 4 at the Workshop on the Economics of Information
 5 Security, which is all about your potential for actually
 6 being injured as a result of a bad actor on the dark
 7 web. And you should go and look at this research,
 8 because it's fascinating, in that these great computer
 9 scientists go out there, and they actually try and work
 10 out, if I'm trying to do identity theft, how do I do it?
 11 And so it's all very interesting.
 12 But what they found out, which really surprised
 13 me, is it's just not a very scalable profession, and as
 14 a result, basically they take so long to do their
 15 identity theft, there tends to be 100 people each time
 16 who are injured, and it doesn't vary as much with the
 17 numbers of records that are left or lost as you might
 18 think.
 19 And so I think, you know, if I was sort of -- as
 20 Lynn is collecting such wonderful data, I think if we
 21 were to really try and have a measure of identity theft,
 22 the risk of it, sort of the first point of measuring the
 23 injury, I would actually like to sort of highlight this
 24 research.
 25 Which talks about the supply side and some of the

246

1 surprising insights that it's not very scalable, which
 2 may explain why sometimes the incidence of identity
 3 theft from a data breach is less than we might think.
 4 MR. SMITH: Thanks, Catherine.
 5 Josephine, any thoughts on these measurement
 6 questions?
 7 MS. WOLFF: So one of the things I think is
 8 really interesting about outcomes -- and I come across
 9 this a lot when I'm both talking to people who sell
 10 insurance and people who buy insurance in this space --
 11 is that outcomes are much easier to tie to an individual
 12 person than to an individual incident.
 13 And so if we're talking about, you know, what
 14 were the consequences of this particular breach with
 15 Equifax or whoever else, that's a very, very hard
 16 question to answer, because your information has been
 17 stolen so many times. Earlier today, they referenced
 18 they think most of the Equifax information had probably
 19 been available on the black market even before that
 20 breach, so it's hard to say this incident of identity
 21 theft or this particular -- even sort of emotional or
 22 psychological toll associated with that was the fault of
 23 this particular company and this particular breach.
 24 It's much easier -- though it's not easy by any
 25 stretch -- to say this is the outcome associated with

247

1 this individual person. This is the amount of financial
 2 fraud. This is the amount of time. All of those things
 3 are easier to measure in terms of people. And the
 4 reason that's important, I think, is because all of our
 5 thoughts and all of our sort of ways of understanding
 6 how policy can come in and try and correct these
 7 externalities have to do with what are the levers, what
 8 are the pressures we apply to the companies and say your
 9 breach caused this amount of damage, which is actually a
 10 much harder question to answer than what were the
 11 outcomes for this individual person as a result of the
 12 sum of all of the incidents that they've been involved
 13 with?
 14 And I think that's a big part of the reason that
 15 we're starting to see a lot of the solutions -- or at
 16 least the insurance market certainly thinks of them as
 17 solutions -- coming to center more on the individual
 18 than on the companies. But I think one of the things
 19 that is perhaps problematic about that is even though
 20 that aligns with the ways that we can perhaps calculate
 21 or collect data more accurately, it means that all of
 22 the entities that have the most power to decide how this
 23 data is being protected are not necessarily the ones who
 24 have the real incentives to be executing that in the
 25 same way.

248

1 MR. SMITH: Thanks, Josephine.
 2 Garrett, do you have any thoughts on this?
 3 MR. GLASGOW: Sure, just briefly. I keep using
 4 the words "easy cases" and "hard cases" if we're talking
 5 about outcomes. I think in some cases it's -- I
 6 wouldn't say easy, but it's easier to measure harm.
 7 I've talked about market transactions with companies
 8 that don't live up to a promise. So, say, for example,
 9 you do business with a company that has a certain
 10 privacy policy. They say we will not share your data
 11 with marketers, but, in fact, they do, and that's the
 12 extent of it.
 13 Measuring the outcome there and measuring the
 14 harm that came from that outcome is pretty feasible. I
 15 think that that's something that we can do. It's sort
 16 of a benefit of the bargain type argument. I paid you a
 17 certain amount. Some of that amount was for you to
 18 protect my data. You didn't live up to your part of the
 19 agreement.
 20 It's the same kind of techniques we would use for
 21 a defective product, say, in a class action case. My
 22 washing machine is leaking. One of the deals is when
 23 you buy a washing machine, it doesn't leak. So you owe
 24 me some kind of compensation for that. One of the deals
 25 when I bought your streaming video service was you

1 wouldn't share my information with marketers. You did,
 2 so you owe me some compensation for that.
 3 Where it gets a lot harder is when we start to
 4 introduce a lot more uncertainty, which is you didn't
 5 sell my information to a marketer, you lost it to
 6 hackers, and it's now on the black market somewhere.
 7 The possible harm that might happen, it could be well
 8 beyond the value of the product. I'm paying \$10 a month
 9 for a streaming video service. If a hacker steals my
 10 information and drains my bank account, that's probably
 11 going to be a lot more harm than \$10 a month.
 12 Now, I will say some researchers have tried to
 13 measure this sort of harm by looking just at the value
 14 of the information, which is how much can you sell
 15 somebody's personal information for on the black market?
 16 What does it cost to buy a Social Security number?
 17 There's actually prices out there. You can buy
 18 someone's information.
 19 I don't think that's a measure of harm. I think
 20 how much a criminal would pay for a record to open up a
 21 fake bank account or take out a payday loan and then run
 22 away, that amount is much less than the harm caused to
 23 the consumer than the criminal is paying for. Just like
 24 if somebody breaks into your car, they break into your
 25 car and they steal your sunglasses, well, you have that

1 loss, plus you have got to fix the window, and your car
 2 is in the shop for a while and so on. There's a lot of
 3 additional harm that's not measured by just looking at
 4 the price that that information can be sold at. So that
 5 I think is the hard case.
 6 Once we introduce this uncertainty -- and we can
 7 measure things like the time spent changing records and
 8 changing passwords and so on, but that's -- I guess I'll
 9 leave it there. There's easy cases and hard cases, and
 10 unfortunately, most of them are hard cases.
 11 MR. SMITH: Thanks.
 12 So, Ginger, I'd like to get your thoughts on
 13 this, but also maybe if you can transition us into our
 14 next question, which is basically this question of
 15 causality. You know, when information has been stolen,
 16 how can we measure the risk and how can we kind of maybe
 17 sort of back out causality, what events may have caused
 18 that, or just get any kind of sort of way to clarify
 19 sort of the harm that happens in these kinds of cases?
 20 MS. JIN: Yeah. I started the panel by
 21 emphasizing the difference between the ex ante
 22 perspective and the ex post perspective. In fact,
 23 estimation on the ex post harm I would say is extremely
 24 important for us to understand the ex ante expectation
 25 of harm, because we want to know what's the financial

1 loss of identity theft, and we also want to know how
 2 many percent of people actually suffer that loss, how
 3 many do not suffer that loss, right? We want to know
 4 the distribution of those losses across the population.
 5 That would give us sort of a big picture distribution so
 6 that we can form an ex ante expectation on this, okay?
 7 But I will say that probably ex post harm
 8 estimation is not enough. We also want to sort of
 9 quantify the risk. I mean, I talk about -- the third
 10 panel, too, also talked about if a firm have risk, that
 11 a firm's data practice would increase, right? If there
 12 is an increase of risk, we want to measure that. We
 13 also want to measure how many people got exposed to that
 14 risk.
 15 So I just want to point you to two sort of
 16 research directions I see as quite promising in doing
 17 that. We know it's very hard to tie back to a
 18 particular firm's data breach or data practice. One
 19 promising direction I have seen is a study by a group of
 20 researchers from Google, from Berkeley and from the
 21 International Computer Science Institute. They actually
 22 studied the dark web, okay? They track -- they are
 23 passively monitoring the dark web for a year, and they
 24 were able to identify 1.9 billion user names and
 25 passwords stolen from the previous breaches.

1 They are also able to -- if you look at their
 2 paper, they are also able to give a list of the top 20
 3 leakages, which identify the companies that got the data
 4 breach and, therefore, got the records on the black
 5 market. So this suggests there is a way to sort of link
 6 a data breach to what kind of records are on the market.
 7 Of course, we need other link from that records
 8 on the market to some real fraudulent transactions or
 9 identity theft or other sort of tangible or intangible
 10 outcomes that eventually happen to consumers, but
 11 obviously this is sort of a good one step forward to
 12 connecting the dots in the dark web.
 13 Another study that was fascinating was about the
 14 blockchain. I think this might be a technology solution
 15 in the trackability of data flows. If blockchain can be
 16 used as technology to track Bitcoins ownership, maybe
 17 that technology could be used here to track sort of how
 18 the data change from one hand to the other.
 19 I'm not a computer scientist, I don't know
 20 exactly how to do that, but I have seen other people,
 21 both computer science and economists, sort of try to
 22 work in this area. To me, it seems pretty promising
 23 direction to really do some research on.
 24 MR. SMITH: Thanks, Ginger.
 25 Lynn?

1 MS. LANGTON: So both Ginger and Josephine made
 2 the point that, you know, causal ordering is really
 3 difficult to establish when you're talking about
 4 individual incidents, and I would certainly echo that,
 5 and it's something that we've wrestled with quite a bit
 6 with the supplement. Are there ways that we can more
 7 directly try to tie experiences of data breaches to
 8 individual incidents of identity theft?
 9 And the reality is, I mean, when you're
 10 collecting survey data, the data are only as good as the
 11 responses you get, and we know, because we already ask
 12 respondents if they know how their information was
 13 obtained, that the majority of victims don't have any
 14 idea. So we have about 30 percent of our victims that
 15 say they have some idea, even if they're not sure, about
 16 how their information was obtained.
 17 So, you know, using a survey like the NCVS to try
 18 to get at this causal relationship between data breaches
 19 and identity theft is really not the best vehicle,
 20 unfortunately. I think you have to look for sort of
 21 these other technological, computer science-based
 22 solutions.
 23 I mean, among those that do say they know how
 24 their information was obtained, about 20 percent of our
 25 victims say that it was obtained through personnel or

1 other files, personal information being obtained through
 2 a company that had their information, but, again, that's
 3 such a small percentage of the 30 percent that knew how
 4 their information was taken that we can't really use
 5 that to draw any conclusions. The causal ordering issue
 6 is a big problem for that.
 7 MR. SMITH: Thanks, Lynn.
 8 Catherine?
 9 MS. TUCKER: Oh, no, I just -- I think, you know,
 10 Ginger and I completely actually agree in that, you
 11 know, what she was saying is that to measure a causal
 12 link, we have to have a better understanding of what
 13 actually causes injury to happen, and I think if you
 14 look at, you know, too much of research, we're trying to
 15 come up with an average effect rather than understanding
 16 what leads to those few incidents which are really bad
 17 that happen. So I think we're in agreement. I don't
 18 need to take any time.
 19 MR. SMITH: Great.
 20 Josephine?
 21 MS. WOLFF: I would just say I think the flip
 22 side of that, which is also an important area for more
 23 research both from academia and from government and
 24 industry, is what prevents harm from happening, which I
 25 think is also a pretty underdeveloped area.

1 To take two examples that you have probably
 2 encountered, one are the chips in your credit cards
 3 where we had a big liability shift in this country a
 4 little more than two years ago about the kinds of credit
 5 cards you use and implanting those microchips in there
 6 to help prevent future data breaches from being able to
 7 steal those numbers as easily.
 8 Another one you have probably encountered at some
 9 point is multifactor authentication, maybe for some of
 10 your accounts now you log in not just with a password
 11 but with another code or a tap on your smart phone or
 12 something, and I think that trying to understand what
 13 the impact of those types of defenses actually is in
 14 practice, right? Does it actually cut down the harm?
 15 Does it cut down the number of data breaches? Does it
 16 cut down what the injuries look like when data is
 17 stolen?
 18 I think we have a long ways to go still in trying
 19 to understand which of these different mechanisms
 20 actually work for preventing the types of harm we care
 21 about, and especially if we're moving away from being
 22 able to hold companies liable directly for things like
 23 identity fraud, because it is going to be hard to trace
 24 back to individual breaches, I think being able to have
 25 very clear expectations about what the ex ante

1 protections should be, based on empirical evidence, is
 2 going to be really important in that space.
 3 MR. SMITH: Thanks, Josephine.
 4 Garrett?
 5 MR. GLASGOW: Sure. Just briefly, I think if we
 6 are going to understand the -- understand causality and
 7 understand the increase in risk from any particular data
 8 breach, we need to understand the baseline risk, and I
 9 don't think we have a good handle on that right now.
 10 The Identity Theft Resource Center has reported
 11 over 8,000 data breaches this year alone, more than 20 a
 12 day. Some are large, some are small, but there is this
 13 constant background of leaks of information out there,
 14 and it's perhaps impossible at this point to know, if
 15 your information shows up in some identity theft case,
 16 where exactly it came from.
 17 To apply this to my -- I have this same analogy
 18 of privacy as Prince William Sound and the Exxon Valdez
 19 spills oil there. Maybe imagine we go -- Exxon Valdez
 20 runs aground, spills oil, the cleanup crews show up, and
 21 it turns out 20 other tankers ran aground there
 22 overnight and were towed away by the owners, but left
 23 all the oil behind, so, you know, how much damage did
 24 the Exxon Valdez do if it spilled oil where 20 other
 25 tankers have already dumped a whole bunch of oil?

1 Maybe that's a really negative viewpoint, but,
 2 you know, when we talk about the intrinsic value of
 3 privacy, maybe that value has been severely eroded by
 4 the sort of permeating background of radiation and
 5 continual data leaks, and that's one thing I think we
 6 need to get a handle on, is what's out there, how maybe
 7 in the aggregate we can see identity theft increasing,
 8 but, you know, how much of this is due to breaches six
 9 months ago? a year ago? We just don't know. So we
 10 don't have a good handle on baseline risk, and that
 11 makes it very hard to establish causality or increases
 12 in risk.

13 MS. CONNOR: This has all been incredibly
 14 interesting, and we have a few audience questions. The
 15 first one actually I think could implicate both consumer
 16 preferences and revealed preferences or stated versus
 17 revealed, potentially.

18 So the question is, are you considering studying
 19 the increase in purchases of ID theft products or cost
 20 for freezes, lifting freezes, delays to obtain credit
 21 while waiting for a freeze to be lifted?

22 And I don't know if anyone, in particular, would
 23 like to take a first stab at that.

24 MR. SMITH: I think the question could just be
 25 rephrased as would that be a way to get some kind of

1 measure of how much consumers value or how much they're
 2 harmed from ID theft?

3 MS. WOLFF: I think that's possible. I think one
 4 of the things that's complicated about purchases of
 5 those products is that most people who have them have
 6 them through a breached company. So the people who are
 7 usually sort of the big purchasers for those are the
 8 entities that get breached, who then purchase a contract
 9 for hundreds of thousands or millions of their
 10 customers, and it's then usually offered free of charge
 11 for at least a period of time to those individuals.

12 So there's some interesting work to do sort of
 13 looking at how many people actually take the company up
 14 on that offer and how that's changed over time, but I'm
 15 not sure it's exactly an economic decision on the part
 16 of the individual consumer.

17 MS. CONNOR: And, Josephine, I wonder if your
 18 answer changes when you're talking about personal cyber
 19 security insurance. I know you discussed it quickly at
 20 the beginning, but I know I didn't really know about it
 21 before I spoke to you for the first time, so maybe you
 22 could kind of explain it and whether or not a
 23 measurement of that would really change your answer to
 24 this question.

25 MS. WOLFF: I think that it could. I think at

1 this point, when we talk about personal cyber insurance,
 2 we're talking about probably about tens of thousands of
 3 people in this country, so it's a very, very small
 4 population of people who have actually purchased these
 5 policies. They are mostly fairly high net wealth
 6 individuals, so it's not something that low-income
 7 people are looking around to purchase or even most
 8 middle-income people are looking at.

9 I do think it's a different measure because it is
 10 something that people are paying for out of pocket. So
 11 it is them deciding, you know, this is a type of risk
 12 I'm concerned about, and I want to have some protection
 13 from all of these different ways of thinking about it.

14 I think the other reason it's interesting is if
 15 you look at how those policies are being structured, at
 16 least right now, they encompass a lot of things that I
 17 at least would not necessarily have associated as risks
 18 of sort of computers and cyber security. For instance,
 19 we're seeing families purchase insurance to cover home
 20 schooling costs in the event that their children are
 21 cyber bullied and don't want to continue going to
 22 school.

23 So I think it's this very complicated set of
 24 costs that's totally dictated by what people want and
 25 are willing to pay for as opposed to what we think the

1 company should be responsible for protecting you
 2 against, and that when you shift the question and you
 3 say, okay, what is it that we think people are actually
 4 willing to spend money on, it turns out there are a lot
 5 of different kinds of harm or injury that people might
 6 be interested in trying to insure themselves against and
 7 that at least some people are willing to spend money on,
 8 which I think does give you a sense of what people
 9 really care about and want to protect themselves
 10 against, but, again, at this moment, we're talking about
 11 a fairly small population.

12 MS. CONNOR: Okay, great.

13 And we have another question, and maybe,
 14 Catherine, given that you opened up talking about data
 15 breach notification laws, you might want to take a first
 16 stab at it, but the question is, can panelists discuss
 17 the multitude of state breach reporting rules and how
 18 that complicates setting a national standard of harm or
 19 injury?

20 MS. TUCKER: Well, I'll just start off by saying,
 21 so as part of this study we did about hospital data
 22 breaches and data breach notification rules, we spent a
 23 lot of time trying to decode the different texts of the
 24 laws, and there's an amazing amount of variation.

25 And the other thing I would say is that in my

261

1 very lay opinion, many of the laws seem rather
2 inconsistent if you know anything about technology, in
3 that there were exemptions which make no sense, and it
4 looks like, I don't know, people, you know, were just
5 sort of taking a random word generator sometimes to
6 actually try and describe what they wanted to happen.

7 Now, maybe this is an opportunity for something
8 better, but certainly I had a certain amount of
9 disquiet, having seen the lack of standardization in
10 these laws, and I'm an economist, not a lawyer, you
11 know, so that's probably a bad thing.

12 MS. CONNOR: Ginger?

13 MS. JIN: I think given the discrepancy we see
14 across states, there is definitely a value to
15 standardize the notification law just to make sure that
16 firms know what to do after a data breach, but I want to
17 ask probably a harder question, that we've got a concern
18 about what happens after notification, okay, if the
19 firms sort of meet all the obligations stated in the law
20 and have disclosed the information they know at that
21 moment.

22 And so what -- that's -- we're relying on the
23 consumers or the media or the public somehow respond to
24 it, so that they would feel embarrassed and, therefore,
25 improve their data security? I mean, that's -- to me,

262

1 that sounds like a pretty wishful thinking. As we know,
2 if sort of the harms we have in mind cannot be traced
3 back to the individual firms, and they already done
4 their duty in notification, it's almost like, okay, I
5 have done what I can, right? The rest is up to you.

6 So it's up to the consumers and the vigilance of
7 sorting having their own preventive measures or other
8 things. I think that question has got to be coupled
9 with about the data notification law itself.

10 MS. CONNOR: Did anyone else have any thoughts on
11 that question?

12 MR. GLASGOW: Just on reporting requirements in
13 general, I'll say, you know, of course, we want -- if
14 companies lose control of our data, of course, consumers
15 need to know about that, but I think -- I have nothing
16 in particular to say about any particular state's
17 requirement, but one thing that we have looked at at
18 NERA is the correlation between media coverage and both
19 class action lawsuits and enforcement actions.

20 If your case goes viral, you can expect lots of
21 class action lawsuits, and you can expect a lot of
22 attention from regulators. So I think one thing we
23 might want to think about is are we creating any
24 perverse incentives with the way that these disclosure
25 laws are written? Do companies want to try to game

263

1 them, to try to do things to minimize media coverage or
2 meet the letter of the law without providing any
3 information that can be seized upon by the media?

4 It's something that -- I mean, I'm not sure that
5 we have created a perverse incentive, maybe it's just
6 one of those things that goes viral sometimes or the
7 biggest cases tend to pick up the most coverage, but
8 that is one thing that I know that a lot of people in
9 the industry are aware of, is the data breach is bad
10 enough, but if the media gets wind of it and then the
11 class action lawsuits and the enforcement rolls in,
12 that's a whole bunch worse. So that's one thing to
13 think about in terms of what kinds of reporting we
14 require and how we require that reporting.

15 MS. CONNOR: Okay, thank you.

16 Well, we have a few minutes left, so I think as a
17 final topic, we would love to hear what you all think
18 should be the focus or the focuses of research on
19 informational injury going forward.

20 And I know you have sort of answered this in your
21 answers already, but maybe specifically what should
22 researchers and the government work on to improve our
23 ability to measure and assess informational injury. And
24 maybe this time we will start at the opposite end of the
25 table, so Josephine.

264

1 MS. WOLFF: I'm trying to think of a new answer
2 that we haven't touched on. One thing that we haven't
3 talked a lot about that I think is important for an
4 agency like the FTC is thinking about sort of which
5 injuries people have some protection from, right? So
6 back when data breaches were mostly about payment card
7 information, we had a lot of policy protections in place
8 to say, if somebody's using your credit card
9 fraudulently, you're not going to be liable for at least
10 most of those charges, usually any of those charges,
11 because your bank and your payment card network are
12 going to want to keep your business. They are going to
13 want to cover that for you.

14 Now, as we have seen, say, a strong shift towards
15 ransomware and other types of cyber crime that are
16 hitting individuals more directly, that they have less
17 insulation from the direct economic costs of, I think
18 there's an advantage there that sometimes it's easier to
19 calculate those costs, because if you're talking about
20 something like ransomware, you can put a price tag on it
21 more directly.

22 But there's another question that comes up about
23 how much do you sort of weight the fact that individuals
24 are going to be bearing those costs directly and does
25 that change the kind of injury or the kind of remedy

1 that you want to have in place, depending on why that
 2 ransomware infected my computer in the first place and
 3 was it my fault or should my ISP have had some inkling
 4 of that, and how the question of sort of distributing
 5 the costs in that way is going to change the incentives
 6 of the large, centralized, powerful actors who might
 7 have the most potential to implement widespread security
 8 controls or defenses?
 9 MS. CONNOR: Thank you.
 10 Catherine?
 11 MS. TUCKER: Well, so, if I've got to say what
 12 you have got to research, it's just like a wonderful
 13 thing to be asked. I think I would flip the focus of
 14 research in that there's a very natural tendency to try
 15 and think, well, how can we measure most accurately an
 16 average effect? I might encourage you instead to focus
 17 on the question of how can we identify the occasions or
 18 incidents or people where there is no injury, where
 19 there is no effect, because I worry that we may be going
 20 towards a world -- which is very natural to try and
 21 understand how do we measure an average from average
 22 baselines and so on -- but I think this is such an
 23 intriguing field because so oftentimes we don't see
 24 injury, and trying to understand and pinpoint those
 25 occasions seems to me incredibly both exciting and

1 valuable.
 2 MS. LANGDON: Interesting perspective.
 3 So I think there have been a lot of issues raised
 4 today about how we can measure different aspects of data
 5 security and the harms associated, and in some ways, the
 6 NCVS, the National Crime Victimization Survey, is
 7 limited in that it can't address these full range of
 8 topics that we would want to measure and harms that we
 9 would want to measure, but I think as a government
 10 researcher, we want to try to measure as best we can
 11 what we can measure.
 12 The thing that we can do is look at level and
 13 change over time in terms of identity theft, which is
 14 obviously a direct harm, and then we also have another
 15 supplement that I'll just make the pitch for that we
 16 just implemented, it's in the field right now, looking
 17 at financial fraud, which is another potential outcome
 18 of a data breach.
 19 And so just to be able to track over time whether
 20 we're seeing any changes in the prevalence of these
 21 particular types of outcomes that we know are
 22 correlated, though we can't look at the direct causation
 23 and the direct causality to data breaches, but we know
 24 that there's still a correlation there, and to see if
 25 the risk of experiencing some of these outcomes and the

1 nature of some of these outcomes is changing over time.
 2 So that's really what our focus is right now. We
 3 will be putting out data from our 2016 identity theft
 4 supplement in January, and then also in January, our
 5 2018 supplement goes in the field. So, again, we're
 6 trying to measure this consistently over time so that we
 7 can track those trends.
 8 MS. JIN: So one thing we haven't touched much on
 9 in this panel but has been touched in the previous panel
 10 is some similarity between the problem of privacy data
 11 security and the problem we have seen before in, say,
 12 food safety, drug safety, product liability, and tort
 13 laws, and so I would like to see probably more
 14 interdisciplinary research to sort of summarize the
 15 lessons we have learned from those areas and to see to
 16 what extent we can sort of apply the insights we have
 17 learned from those to the market of privacy and data
 18 security.
 19 MS. CONNOR: Thank you.
 20 MR. GLASGOW: And I think an important topic that
 21 isn't well understood, yet that we should push forward
 22 on, is maybe a theoretical or definitional issue of what
 23 we mean by informational injury. Does informational
 24 injury spring from the content of the information itself
 25 or is it how it's treated by, say, a company that you're

1 doing business with?
 2 You know, so here's a thought experiment.
 3 Suppose you're doing business with a company and they
 4 have a data breach and some of your personal information
 5 is stolen and is now out there on the black market, but
 6 then you find out the previous week there was another
 7 data breach with a different company and all that same
 8 information was already out there a week ago. Were you
 9 harmed by that second data breach or not?
 10 And whether or not you were harmed might depend
 11 on what you think of as informational injury. Is it the
 12 fact that this information is now out there? If that's
 13 the harm, the harm is already done. Or is it this
 14 company is mistreating customer data and is not being
 15 fair to customers, is dealing unfairly, maybe that's a
 16 different kind of informational injury, and in that
 17 case, you could be harmed twice by the leak of the same
 18 information.
 19 Both of those things could be sources of harm.
 20 It's entirely valid to believe they are both sources of
 21 harm, but I think that's something that is important to
 22 distinguish when we think about what kinds of
 23 enforcement we want to do and what kinds of harm we're
 24 trying to measure.
 25 MS. CONNOR: Thank you, everyone. It looks like

269

1 we are pretty much out of time, unfortunately, but thank
 2 you to our panelists for such a great discussion and a
 3 wonderful way to end the day.
 4 Andrew Stivers will be coming up shortly to give
 5 the closing remarks. So thank you.

6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

271

1 stuck this limit on me -- to go into all the really
 2 interesting and important topics that were discussed
 3 today, so I want to pick sort of one issue from each of
 4 the panels to highlight, to leave you with, and that
 5 doesn't mean that these are the only things that you
 6 should pay attention to. I'm sure everyone has their
 7 own favorites, but these are things that called out to
 8 me and hopefully will help continue the conversation and
 9 the research that is clearly needed.

10 So the first thing, on the first panel, that I
 11 thought was incredibly good, especially for the FTC, is
 12 we're experts in markets. That's our mission. Our
 13 mission is to make sure that markets work for consumers.
 14 We have over 100 years of grappling with these issues,
 15 both on the consumer protection and the antitrust side
 16 of the house. So we really understand the kinds of
 17 injuries that occur contained within the marketplace.

18 But what's really interesting about data security
 19 and privacy is we see that this -- there's this flow
 20 between commercial applications and personal and private
 21 and social applications that muddy those waters a little
 22 bit, and in the first panel, they noted a variety of
 23 fallouts from the commercial space, the collection of
 24 data for commercial purposes into the personal and
 25 social space that cause these harms that are incredibly

270

1 CLOSING REMARKS
 2 MR. STIVERS: Well, I'm disappointed to discover
 3 that they just -- they noticed the flaw in the agenda
 4 and actually put an end time to my closing remarks. In
 5 the earlier agendas, it was 4:45, that's when I start,
 6 no ending, but somebody discovered that, and they know
 7 me, so...
 8 But most of you don't know me. I'm Andrew
 9 Stivers. I'm the Deputy Director For Consumer
 10 Protection in the Bureau of Economics at the FTC, and
 11 what that means is I head up the consumer protection
 12 mission for the Bureau of Economics. And the Bureau of
 13 Economics, in terms of our consumer protection mission,
 14 we advise the Commission on its actions and its
 15 policies, and we do economic research to help increase
 16 our understanding of the market practices that help or
 17 hurt consumers.
 18 So from that perspective, this has been
 19 incredibly interesting to me, and each of the panels has
 20 built beautifully on the previous one, and I sort of
 21 felt like, wow, they are not going to be able to top
 22 that, and the next one comes up, and they, you know,
 23 reveal all sorts of great issues that we need to grapple
 24 with.
 25 I, unfortunately, don't have time -- because they

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

272

1 important and that we need to grapple with as a society.
 2 The other way is also true, that we see personal
 3 and social transactions, conversations between people,
 4 that because they're mediated through commercial
 5 information products or because those conversations are
 6 able to be monetized in some way, it really creates some
 7 complications for how we think about injury.
 8 So an example of the latter would be in terms of
 9 our work in revenge porn. So there are these terrible
 10 interactions between former intimate partners, and that
 11 transaction, that kind of information being broadcast or
 12 those harms being visited are sort of amplified by the
 13 commercialization and the ability to monetize that
 14 information on some of these sites.
 15 The upside for us, of course, is that we can
 16 actually go after that because it's in a commercial
 17 space. So I think that was really incredibly important
 18 for that first panel and highlights some of the research
 19 and thinking that really needs to continue.
 20 The second panel in my mind really highlighted
 21 the definitional issues. So there were some
 22 hypotheticals put forward. The panelists had often very
 23 different reactions to the hypotheticals and sort of how
 24 they thought about those things. Some of those
 25 reactions to me seemed to be based on definitional

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

1 problems.
 2 So Paul, right at the very end, at least tried to
 3 articulate a definition of what he was thinking about
 4 with injury. The moderators tried to say, no, no, you
 5 know, this is what we're thinking about, but sort of our
 6 interaction in this space or our place in this space
 7 often really informs what we think of as injury, what we
 8 sort of privilege as injury, and what we don't.
 9 And so I think we need to do some more work in
 10 making sure we understand what it is that we're talking
 11 about, and I'll highlight one issue here. Is Geoff
 12 still here? I hate to call him out. This is the one
 13 thing I am going to kind of harp on a little bit. He
 14 said that risk was not injury. If that's true, somebody
 15 needs to tell the insurance industry that they have got
 16 it all wrong, because insurance is exactly about
 17 offering people the opportunity to mitigate a future,
 18 potential, unrealized outcome ex ante, before it
 19 actually happens.
 20 So people are willing to take expensive actions
 21 to mitigate a future outcome, a potential future
 22 outcome. So to give Geoff his due, I think he was
 23 really thinking about, you know, what's the kind of
 24 injury that the FTC should go after? And maybe you
 25 agree with that, maybe you don't, but I think it's very

1 important to think about if a consumer, if anybody is
 2 willing to take an expensive action ex ante to mitigate
 3 the risk of a bad outcome, that's potential risk. If a
 4 firm takes an action, has a practice that motivates me
 5 to go out and spend that money, that's harm to me. So I
 6 think we just need to be a little bit more careful about
 7 how they think about those issues.
 8 And then when we are clear about that, I think we
 9 can really see across the entire panel that was up here
 10 that where we choose to fall in terms of what's an
 11 injury really becomes a policy question, and that's this
 12 whole stew of the questions about, you know, are we
 13 addressing privacy and data security as citizens, as
 14 consumers, as all of the above, or both of the above?
 15 So there's definitely an ongoing policy debate that
 16 needs to continue.
 17 The third panel brought up a variety of
 18 interesting issues, and it was hard for me to pick one
 19 because they -- I think of the panels, they really
 20 covered the broadest range, but the one that I will
 21 highlight, which is one that's really interesting to me,
 22 is this question of internal misuse versus external
 23 misappropriation, right?
 24 So to use an example that I'm familiar with from
 25 some of my past work, when we think about economic

1 adulteration versus disruptive adulteration in the food
 2 industry, right, so economic adulteration is I want to
 3 water down some milk, right? I have a profit motive
 4 there if I'm doing that, and the last thing I want to do
 5 is get caught. So there's going to be some limits and
 6 different incentives in terms of how I approach that --
 7 if I am an adulterer -- that is very different from if
 8 I'm a disruptive adulterer, right? I want to create
 9 some huge disruption in society. I actually want to get
 10 caught. The whole point is to let people know that I've
 11 done this terrible thing.
 12 So it's not an exact analogy, but it at least
 13 highlights that there's very different incentives,
 14 risks, and potential remedies when we think about
 15 internal misuse of the data, internal privacy --
 16 internal to the company uses of the data that somehow
 17 fall afoul of consumer expectations or deception or
 18 whatnot, versus these harms that arise potentially
 19 because the firm has collected this data and not secured
 20 it, but is really being mediated through these outside
 21 actors, these criminal actors.
 22 So we need to think very carefully about what the
 23 incentives are here, what possible remedies might be put
 24 in place, and the liability associated with these
 25 things.

1 Lastly, the final panel -- and I could just
 2 applaud again, because as an economist, this was
 3 exciting and really good and points to all sorts of
 4 really interesting and important research challenges
 5 that we need to grapple with, and I hope that you folks,
 6 as you have access to research skills and funding,
 7 really try to push the envelope on -- but I will kind of
 8 sum up some of what I heard that highlights sort of the
 9 really important research questions and measurement
 10 questions that we have here.
 11 We need to know the kinds of injuries, the kinds
 12 of actions and outcomes and practices that we're dealing
 13 with here, and I think we addressed that in some of the
 14 earlier panels, and we're getting a better sense all the
 15 time of what this looks like, but we need to be able to
 16 measure that pretty carefully.
 17 We need to measure the severity and the impact of
 18 these outcomes. That has all the complications that the
 19 panelists today talked about. We need to know the
 20 incidence of outcomes. That was discussed as well. But
 21 we also -- and this was touched on, but sort of the last
 22 two points are, I think, of equal importance -- we need
 23 to know what confidence we have in the causal link
 24 between the practices that we're attempting to address
 25 and the outcomes to consumers.

277

1 So the more confident that we are that there's a
 2 link between those practices and the particular
 3 outcomes -- or even the practices and a risk of a
 4 particular outcome -- the better off we're going to be.
 5 So in the world of, say, drunk driving, we have really,
 6 really good data on the risks associated with drunk
 7 driving, right? So we are very confident that there is
 8 a causal link between an increased risk of death and
 9 drunks on the road.
 10 Now, there's a really small probability that
 11 you'll actually die in an accident that's caused by a
 12 drunk driver, but the causality in terms of the increase
 13 in the probability, in terms of the risk, is really well
 14 understood, because we have really good data, and we
 15 have been collecting data for a long time. We need to
 16 make sure that we have as much confidence as we can get
 17 in the causal link between the practices and the
 18 outcomes.
 19 And the final thing that I'll mention here is we
 20 need to have some sense of what the market incentives
 21 are. Do we think that the market is going to take care
 22 of a problem? Do we think that there are incentives in
 23 the market for actors to mitigate the risks, to somehow
 24 prevent these harms from occurring, or at least mitigate
 25 them to the extent they can be, or is there some sort of

278

1 market failure that would really call for a regulatory
 2 approach?
 3 So I want to thank the panelists. I want to
 4 thank all of the participants for lending your time and
 5 your expertise to this endeavor. We continue to improve
 6 our understanding, and we want to continue to mine your
 7 expertise. So to that end, there is a 45-day comment
 8 period, and it's going to be ending, I think, January
 9 26th -- is that correct? -- okay, thank you, so that
 10 ends January 26th, and I encourage your input. You can
 11 go to the FTC website to find information about how to
 12 submit your comments if you're interested in that.
 13 Remember that our conference highlighting new
 14 research in the privacy and data security area,
 15 PrivacyCon 2018, is coming February 28th. So please
 16 mark your calendars and show up for that. And the other
 17 thing is that PrivacyCon 2019, which I hope will also
 18 happen, is going to be coming up sooner than you think.
 19 We start asking for submissions, assuming we do this, in
 20 the late summer. So if you're inspired to do some
 21 research now, think about how you might apply to get
 22 that research put in front of us for PrivacyCon 2019.
 23 All right. Finally, I want to thank the Acting
 24 Chairman and her staff for pushing us on this issue, for
 25 instigating this workshop, because I think it's been

279

1 fantastic. And one final time, I want to thank the
 2 boots on the ground, the team that put this all
 3 together. Jacqueline Conner -- is she here someplace
 4 still, there she is, waving -- Cora Han, Doug Smith, and
 5 Dan Wood. Thanks very much.
 6 (Applause.)
 7 (Whereupon, at 4:58 p.m., the workshop was
 8 concluded.)
 9
 10
 11
 12
 13
 14
 15
 16
 17
 18
 19
 20
 21
 22
 23
 24
 25

280

1 CERTIFICATE OF REPORTER
 2
 3
 4 I, Susanne Bergling, do hereby certify that the
 5 foregoing proceedings were recorded by me via stenotype
 6 and reduced to typewriting under my supervision; that I
 7 am neither counsel for, related to, nor employed by any
 8 of the parties to the action in which these proceedings
 9 were transcribed; and further, that I am not a relative
 10 or employee of any attorney or counsel employed by the
 11 parties hereto, nor financially or otherwise interested
 12 in the outcome of the action.
 13
 14
 15
 16
 17 s/Susanne Bergling
 18 SUSANNE BERGLING, RMR-CRR-CLR
 19
 20
 21
 22
 23
 24
 25

A				
a.m 1:10 3:3	30:3,21 81:2,19	acting 2:7 6:13,17	146:3 151:8 229:6	adolescent 51:21
Aaron 6:8	110:12,14,17,19	18:16 52:6 68:5	235:15	adopt 203:19
ability 95:13 96:15	110:23 112:13,18	79:2,6 235:16	acute 86:11	adopting 159:3
119:21 136:13	113:5 114:20,23	278:23	Acxiom 142:17	adoption 148:13
137:14 206:18	114:24 116:6	action 12:2 18:24	153:21	195:13
263:23 272:13	132:9 145:11	88:5,10 96:7	ad 76:11,14,16	ads 61:1 71:8,14
able 5:19 14:5 21:1	219:5 276:6	156:18 171:21	146:1 152:12	76:7,8,17 102:19
26:6 37:25 55:19	accident 277:11	184:20 191:4	163:17 165:13	172:21 175:19
57:14 61:22 63:22	accidentally 62:18	213:25 219:22	172:23,24 175:9	176:4 178:8,8,9
63:23 64:20 85:13	64:13	234:16,18,22,24	175:11,16,18	adult 195:1
87:22 89:23 113:5	accidents 169:5,12	237:16 239:25	176:2,6 177:22	adulteration 275:1
117:12 137:13	accommodation	241:15 242:6,8	181:12,17,22,22	275:1,2
145:6,11 148:12	16:18 44:22 47:13	248:21 262:19,21	ad-supporting	adulterer 275:7,8
160:24 167:23	accompanying 39:1	263:11 274:2,4	144:22	adulterous 235:6
187:11,19 189:23	69:16	280:8,12	add 19:9 52:11	adults 41:15,16
224:23 231:15	account 58:18 86:25	actionable 85:21	54:21 122:19	advance 33:24 34:6
244:10 251:24	118:3,14 141:13	117:25 126:17	132:2 156:16	advanced 23:24
252:1,2 255:6,22	160:1 187:24	actions 18:2,21 35:9	178:3 181:8 185:6	170:10
255:24 266:19	212:23 213:8,10	62:3 94:3 199:16	240:18	advances 167:13
270:21 272:6	249:10,21	231:3,14,20 233:5	addition 9:11 73:3	advancing 159:6
276:15	accountability	233:10,15,16	177:1	advantage 135:17
abruptly 169:7	152:9	236:3,7,9,13	additional 55:5	165:21 187:10
absence 108:8,9	accounting 101:22	239:14,20 240:9	91:23 114:8,9	264:18
absolute 20:22	accounts 27:13,16	240:18,19 241:13	180:10 250:3	adverse 78:19 101:8
65:20,21 115:14	27:18,21 54:4	262:19 270:14	address 12:19,21	advertise 39:14
absolutely 47:18	232:14 255:10	273:20 276:12	14:13 29:9 36:7	76:23
52:12 61:21 88:2	accrue 37:23	active 11:6 142:18	43:2,9 48:18,19	advertisements 61:1
118:2 128:18,24	accurately 247:21	actively 232:21	53:14,21,25 56:3	145:7 175:12
132:19 135:4,23	265:15	233:5	64:13 87:24 94:22	advertisers 89:24
139:9 149:19	Accusearch 12:3	activities 33:10	131:23 181:18	advertises 71:3 85:1
150:16 235:21	achieves 174:22	148:6 157:17	233:11 266:7	advertising 31:24
abstracted 89:2	acknowledge 126:12	195:19	276:24	62:8 70:25 80:23
abuse 16:14 40:2	acknowledgment	activity 5:1 20:16	addressed 60:9,10	142:9 144:1,3,8
abused 40:7	125:24	21:10 91:20,24	133:2,3 153:11	145:5,14 146:1
abuser's 41:25	acquire 29:15,16,25	96:2 106:25	276:13	150:14 151:12,14
abusers 31:22 40:25	103:20 118:24	147:20 211:12	addresses 25:22	152:10,18 153:4
41:5,23	acquiring 104:17	227:1	28:9 96:1	156:22 165:12
abuses 25:8	139:2	actor 88:10 133:24	addressing 9:24	171:1,16 175:10
abusive 12:5	Acquisti 68:9 70:14	245:6	274:13	175:23 185:21
abysmal 202:5	72:1 107:18	actors 23:15 26:17	adds 198:15	advise 270:14
academia 254:23	110:12 118:18	62:7,20 68:17	adequately 187:12	advised 5:2
accept 133:7	130:10 188:6	111:14 134:2	adhering 153:6	advocates 9:6 41:9
acceptable 116:21	act 8:19 9:12,13	265:6 275:21,21	adjust 20:17	167:6 177:20
148:22,22	56:11,12,13 78:7	277:23	Admin 116:12	Aetna 48:13,14
accepted 95:8 223:6	95:22 96:4 104:3	acts 8:20 211:19	administrative 3:17	162:17
access 7:23 15:4	105:18 128:14	actual 9:24 52:2	administrator 116:4	affairs 6:12 235:6
16:19 29:20 30:1,2	191:8 200:16,19	73:5 92:8 98:1	admit 92:7	affect 32:7 60:13
	acted 176:17	101:8 103:13	admitted 129:13	93:8 108:11

affirmatively 197:17	42:11 64:12 91:18 171:8 176:24	102:18 181:21	amplify 122:23	237:22 246:16
afoul 275:17	192:19 222:19	algorithmic 16:10 36:12 58:1	analogy 150:21 152:21 160:21	247:10 258:18,23 264:1
afraid 52:7,8,14 53:1,10 55:9 241:15	238:14 255:4 257:9,9 268:8	algorithms 33:4 217:22	182:3 213:22 256:17 275:12	answered 263:20
African-American 107:10	agree 72:5 99:21 104:20 107:20	ALI 167:8	analyses 34:24	answers 76:1 149:13 227:12 228:6,14 239:12 263:21
African-Americans 107:7	118:2,14 119:2 121:13 126:5	aliases 25:21	analysis 10:15 20:6 26:12 34:3 84:13	ante 212:5 213:1,19 214:3 250:21,24 251:6 255:25 273:18 274:2
aftermath 219:15 234:16	139:25 140:1,6 154:7 156:20	aligns 247:20	90:19 109:20 221:3 222:25	Anthony 164:7
afternoon 141:1,5 143:23,24 208:2 208:13	173:6,7 185:5 191:14 199:6	alleged 9:4 39:15	223:5,8 225:11,20 236:15	antidiscrimination 56:9
Agan 106:18	203:21 225:1 254:10 273:25	allegedly 11:19,22	analysts 70:18	antitrust 271:15
age 25:21 100:15 215:6	agreeing 5:5	allied 136:3	analytic 192:14	anxiety 88:15 92:7 92:20 93:9 117:13 134:4
agencies 12:20 22:11 24:10 65:14 200:5 220:3	agreement 8:17 118:2 127:9 248:19 254:17	allocated 131:21	analytical 193:17	anybody 44:9 61:24 64:2 195:25 200:14 274:1
agency 35:3 87:22 94:9 96:14 134:5 134:19 135:13,17 137:11 138:8 198:21 199:8 200:11 206:17 207:2 264:4	agrees 113:15	allowed 45:14 100:2 105:14 106:11 171:23	analytically 185:17	anymore 25:1 47:2 48:3 61:23 65:6 215:1
agenda 142:11 270:3	aground 256:20,21	allowing 9:10 83:4 228:15	analytics 131:17 161:15 171:11,12 205:1,2	anyway 57:12 76:5 107:16 114:11 125:8 137:11 152:22 174:15
agendas 270:5	AGs 24:11	allows 119:5 159:13 209:15 242:24	analyzed 109:16 233:22	AOL 42:11,19 142:12
agents 73:15,15 209:2	ahead 3:24 23:4 86:4 111:25 132:23 137:25 146:21 174:1 180:15	alluded 208:7	analyzing 73:17	apartment 37:25 46:21 48:23 49:8
ages 20:1	AI 217:22	alongside 6:5	and/or 204:3	apologize 60:24
aggregate 70:15,17 70:20 74:8 75:18 81:23 82:6 89:15 89:20,20 93:4 102:17 109:5 257:7	aids 198:17	alternative 242:20	Andrew 2:20 14:8 269:4 270:8	app 31:4 183:25 184:24 189:8,8
aggregated 74:11 75:2 81:24	aiming 191:24	Altman 72:12	Android 192:16	apparatus 87:21
aggregation 82:7 89:7 93:13	airplane 152:25 182:2	amazing 260:24	anger 228:13	applaud 276:2
aggressive 59:12	airplanes 152:23	Amazon 90:21 158:24 181:6 183:4	angry 174:9,12 228:11,14	Applause 6:15 14:18 67:21 140:23 207:12 279:6
aggrieved 227:2	akin 127:18	Amber 6:8	Anne 6:6	Apple 158:24 159:12 183:4 192:17
agnostic 101:24	alarm 4:20 43:16	American 138:23 227:5	announced 7:10 8:14	Apple's 31:4 159:10
ago 40:18 41:3	alarmists 177:21	Americans 56:10	annoyance 17:24 61:19	applicable 122:21
	Alaska 226:24	amount 25:19 56:24 91:24 109:3 120:7 136:19 155:22 172:7 187:9 212:11 226:4 234:20 243:8 247:1,2,9 248:17 248:17 249:22 260:24 261:8	annoyances 60:18	application 11:3 45:11 106:18
	alert 5:1	amounts 9:14 219:21	annoying 60:20	
	Alessandro 68:9 71:25 87:16 88:13 107:17 115:22 121:14 125:19 129:17,23 130:8 132:15 134:8,12 188:6	ample 108:23,25	annualized 164:4	
	Alessandro's 140:8	amplified 51:25 272:12	anonymize 51:20,22	
	algorithm 70:19 74:22 77:19		anonymized 51:23 161:7	
			answer 17:5 55:17 93:16 116:1 132:24 136:16,18 146:23 156:14 160:15,15 175:13 190:12 194:19 195:25 229:20	

<p>applications 171:11 271:20,21</p> <p>applies 38:16 193:16</p> <p>apply 10:20 117:16 117:16 225:19 227:24 247:8 256:17 267:16 278:21</p> <p>applying 45:17 46:3</p> <p>appointments 46:22</p> <p>appreciate 39:18</p> <p>appreciated 179:8</p> <p>approach 7:14 8:21 57:22 65:11,17 127:22 149:18 150:1,12 222:22 226:12 228:18 239:22,22 275:6 278:2</p> <p>approached 39:3</p> <p>approaches 33:11 64:10 203:17 222:24 223:2,4 228:20 240:10</p> <p>approaching 67:1</p> <p>appropriate 13:17 160:17 161:4 203:11,13 204:24 214:3</p> <p>appropriately 11:8</p> <p>apps 31:2,22,25 32:1 188:8 189:3</p> <p>arbitration 167:8 184:20</p> <p>architectures 182:13 183:11</p> <p>area 4:24 6:2 50:18 52:12,25 58:25 60:3 80:16 83:13 107:24 139:8 166:1 185:19 210:16,24 211:9 211:17,25 224:1 228:23 239:21 252:22 254:22,25 278:14</p> <p>areas 8:25 16:3,17</p>	<p>19:23 22:12 33:13 34:13 36:25 97:9 128:16 191:1 202:3 210:15 219:11 225:19 226:17 267:15</p> <p>arguably 95:23</p> <p>argue 166:13 212:13 212:20</p> <p>argued 10:6</p> <p>argument 109:11 130:22 248:16</p> <p>arisen 120:18</p> <p>arising 34:12 39:9 98:2 107:22</p> <p>arm-waving 178:14</p> <p>armored 28:18</p> <p>arrangements 169:2</p> <p>array 15:3 186:24 199:4</p> <p>arrested 18:8,9</p> <p>art 239:6</p> <p>article 199:1</p> <p>articles 35:24</p> <p>articulate 273:3</p> <p>artificial 33:24 193:3,12 205:2</p> <p>artist 238:14</p> <p>ascribe 154:24</p> <p>Ashley 12:12 234:22 235:2</p> <p>Aside 6:2</p> <p>asked 80:7,8 171:21 178:17,18 217:5 229:10,15,18 240:22 243:14,16 265:13</p> <p>asker 60:23</p> <p>asking 17:4 117:25 173:12 226:15 229:24 231:23 278:19</p> <p>asks 133:6 216:8,10</p> <p>aspect 45:9 168:5 184:14</p> <p>aspects 15:9 84:1 95:10 167:5 197:11,20 204:24</p>	<p>204:25 266:4</p> <p>assault 62:17 64:21 127:2</p> <p>assaulted 39:25 40:1</p> <p>assembly 4:24</p> <p>assertion 172:17</p> <p>assertive 179:23</p> <p>assess 90:24 128:12 128:12 132:12 147:5 161:23 187:11,12,20 189:15,16 208:9 263:23</p> <p>assessing 2:12 7:25 12:13 13:10 51:6,7 68:1 125:21 132:7</p> <p>assessment 100:1,20 112:3 127:4 129:1 129:2 148:19 161:21 190:17 196:12</p> <p>assessments 148:17</p> <p>assignments 47:3</p> <p>assistant 16:1 209:20</p> <p>associate 68:3 70:20</p> <p>associated 12:11 124:2 215:25 233:23 243:4 246:22,25 259:17 266:5 275:24 277:6</p> <p>associates 71:4 85:1 85:9</p> <p>Association 154:16</p> <p>associations 144:21</p> <p>assume 78:10 112:19,20,23 216:20</p> <p>assumes 80:21</p> <p>assuming 85:10 278:19</p> <p>assumption 81:14 112:11,12</p> <p>asymmetric 140:11</p> <p>asymmetries 109:7 128:23 138:21 140:7</p>	<p>asymmetry 112:17 131:14 209:2</p> <p>at-home 155:8</p> <p>AT&T 194:7</p> <p>attached 94:18 96:7</p> <p>attack 30:17</p> <p>attacked 30:22</p> <p>attacker 30:5,8</p> <p>attackers 30:17,18 30:18,21</p> <p>attacks 24:14 32:11</p> <p>attempt 53:24 197:25</p> <p>attempting 276:24</p> <p>attempts 38:24 51:22 53:4 64:17</p> <p>attention 162:6 206:13 262:22 271:6</p> <p>attorney 3:10 16:15 17:1 18:13 44:6 280:10</p> <p>attributable 214:6</p> <p>attribute 90:6</p> <p>attributed 14:2</p> <p>attributes 35:16 79:6 216:7 223:12 223:13</p> <p>audience 3:20 5:13 5:20 15:15 60:7,8 69:17 123:13 132:22 154:17 195:23 257:14</p> <p>audiences 184:17,18</p> <p>auditing 200:11</p> <p>auditorium 4:2,11 5:16,17 15:17 141:20</p> <p>Audits 200:11</p> <p>authenticated 23:13</p> <p>authentication 23:17 255:9</p> <p>authentications 23:16</p> <p>author 142:24</p> <p>authority 112:6 200:16</p> <p>authorizing 137:11</p>	<p>auto 168:25 169:11</p> <p>automated 34:16 36:4 37:13,19 195:20</p> <p>automatically 27:11 149:23</p> <p>automotive 16:6</p> <p>autonomous 185:2</p> <p>autonomy 38:17 78:3 104:2 109:18 130:12</p> <p>available 5:8,11,14 56:2 132:8 141:19 150:5,8 160:24 161:17 186:25 191:23 223:19,21 223:25 246:19</p> <p>average 191:17 254:15 265:16,21 265:21</p> <p>aversely 218:13</p> <p>avoid 72:10 128:19 146:11 233:5</p> <p>avoidable 128:14,17</p> <p>avoided 145:18</p> <p>avoids 65:18</p> <p>aware 3:21 37:12 72:22 99:5 112:13 112:14 113:4 155:10,15 157:12 165:2,9,20 170:3,9 170:9 237:14 263:9</p> <p>awareness 81:3 82:24 92:24 113:3</p> <p>AWS 185:9</p> <hr/> <p style="text-align: center;">B</p> <hr/> <p>B 185:25</p> <p>baby 54:12 76:16</p> <p>back 3:23 18:14 33:1 39:11 40:19 40:23 46:9,14 57:4 67:20 73:25 84:11 91:8,10 92:9 95:3 98:25 105:3 106:25 107:24 108:17 110:4</p>
---	---	---	--	---

112:4 119:5 127:1 129:14,15 130:2 131:12 133:9 141:6 147:24 148:11 173:9 180:1,7 186:1 189:16 190:5 192:7 196:11 202:11 213:4,13 213:14 214:8,16 221:8,23 250:17 251:17 255:24 262:3 264:6	bank 53:18 232:7,10 239:8 249:10,21 264:11 bar 106:1 107:5 Barbara 222:20 bargain 168:13 248:16 barista 40:10 Barker 6:8 barred 186:14 base 105:11 152:7 based 20:16 21:22 21:22 23:12,21 26:5,11 33:23 35:16 36:4 45:24 57:14,16 58:5 63:15,16 73:16 78:12 79:5 94:11 105:14 107:14 190:12 200:13 206:19,21 226:5 256:1 272:25	184:24 befall 88:15 92:1 befalling 94:11 beginning 51:3 84:7 161:4 258:20 begins 67:14 70:15 70:17 81:8 93:4 behalf 3:5 behave 197:25 217:17 230:7,18 230:20 240:7 behaved 198:12 behaving 118:8 behavior 18:11 59:4 94:21 106:3 117:15 178:4 229:6 240:3 behavioral 80:23 140:11 175:23 behaviors 9:4 72:23 103:24 216:11 231:23,25 232:25	168:17 169:14,20 169:21 172:15,19 202:22,22 248:16 benefited 137:3 benefiting 119:23 benefits 8:2 9:8 10:3 10:7,9 13:19,23 16:20 34:12 73:16 86:1 88:24 99:15 103:19 104:2,7,7 104:16 105:22 107:22 119:24 128:15 132:16 141:9 143:20 144:4,5,25 145:19 146:10 147:7,14 149:2,4,8 160:2 164:21 168:20 169:23 170:17 183:18 202:21,24 231:8 235:19	biased 52:20 178:15 biases 35:1 51:7 140:10,12 big 16:8 34:11,13,15 48:19 50:1,3,4 58:25 75:15 83:11 97:7 122:25 125:15,18 133:9 140:4,5,13 144:24 158:23 159:22 164:3 171:11 174:15 175:1 182:19 183:3 185:16 202:25 205:22 214:21 218:9 220:16 226:23 247:14 251:5 254:6 255:3 258:7 bigger 151:15 biggest 34:13 191:25 214:4 231:4 241:1 263:7
back-and-forth 69:3 69:8 backbone 151:13 backdrop 93:20 backed 122:20 background 256:13 257:4 backlash 191:7 backward 97:20 backwards 134:6 bad 18:10 23:15 49:8 62:7,20 68:16 68:17,17 111:12 111:14,15 133:23 136:8 156:12 170:2 174:10 186:12,14 189:4 211:19 213:16 226:16 241:9 245:6 254:16 261:11 263:9 274:3 badge 4:13,15 baggage 71:23 baked 58:23 238:14 bakes 210:23 balance 103:9 139:24 148:8 153:9 balances 188:24 balancing 104:9 139:23 ball 21:25 ban 106:8,13,20 107:5,9	baseline 124:9,17 126:10,20 128:3 256:8 257:10 baselines 128:2 265:22 basic 152:7 168:4 232:4 basically 25:15 29:24 51:18 106:16,20,20 137:13 143:16 168:24 229:3 241:6 245:14 250:14 basing 234:4,4 basis 164:4 185:13 226:2 Bayesian 123:14 133:16 be-all 95:6 bear 3:24 53:18 135:25 bearing 264:24 beautifully 270:20 becoming 27:16 43:3 155:2 165:20	behooves 92:12 94:12 beings 39:14 beleaguer 60:18 believe 12:23 15:18 38:4 45:19 80:1 108:6,7,16,20,21 131:17 140:21 159:2 204:22 214:2 231:7 239:20,21 268:20 belly 176:4 Ben-Shahar 141:25 166:20 177:11 183:21 188:3 193:24 197:1,7 201:14 benchmark 24:23 beneficial 104:6,19 119:15 benefit 8:21 13:18 28:1 63:3 80:17,22 80:25 81:1,18 86:9 86:18 118:13 144:13 147:13 148:23 158:3	benign 134:3 Berbling 1:25 280:4 280:17,18 Berkeley 251:20 Berry 6:7 best 3:25 5:20 58:20 67:19 83:2 112:6 150:11 161:22 205:13,16,20 253:19 266:10 bet 67:19 88:20 better 7:11,16 12:21 13:25 28:23 55:12 100:6 104:21 105:19 126:19 140:15,19 158:9 175:25 191:6 201:2,4,4 218:11 240:2 254:12 261:8 276:14 277:4 beyond 17:11 43:25 98:19 115:15 156:1 188:23 243:1 249:8 bias 34:7 50:25 51:14	bill 19:2 billing 18:23,23 21:17 23:1 billion 251:24 binary 181:20 biometric 21:24 22:2,6,12 23:3 24:12,14,21 25:5 50:2 65:2,5 biometrically 23:16 biometrics 22:16 bios 68:8 birth 25:21 47:21 53:17 177:3 bit 20:15 25:7,13 32:25 36:10 39:20 45:12 52:1,3 55:23 56:1 68:15,19 78:1 81:8 86:3,25 91:20 92:4 115:6 130:1,2 144:17 158:14 165:16,24 166:1 171:3 180:8 183:17 190:5 210:3 219:23

<p>222:14 228:4 233:11 253:5 271:22 273:13 274:6 Bitcoin 229:11 240:20,23 Bitcoins 252:16 Bitdefender 192:1,3 BJS 215:4 black 131:18 213:7 239:11 246:19 249:6,15 252:4 268:5 Blackman 6:7 blatant 45:25 62:20 blazing 28:19 blend 115:6 block 51:20,22 172:23,24 175:11 blockbuster 115:14 blockchain 252:14 252:15 blocker 177:22 blockers 175:11,18 blocking 175:9,16 176:6 blog 40:18 blood 46:8,24 blue 11:12 211:1 Bluetooth 191:19 blurrier 139:1 Bob 142:21,21 149:11 154:7 173:25 174:1,21 176:13 188:19 191:12 193:24 196:19 204:20 Bob's 206:6 body 140:8 214:1 boil 32:4,7 38:24 boiled 188:9 book 18:5 142:24 206:6 books 35:23 boots 279:2 born 47:20 borne 132:19 boss 40:9 78:24,24</p>	<p>78:25 105:1 bosses 105:14 bottom 159:21 bought 77:13 82:4 86:6,13 93:6 157:2 157:3,3 248:25 boundaries 72:16 118:21 217:23 boundary 72:14,25 73:1,12 129:24,25 box 106:8,14,20 107:5,9 131:19 boxes 95:2 198:13 boys 40:7 brand 150:7 brandish 166:23 breach 12:12 35:7 62:14 113:15 120:20 122:3,13 123:11,19,21,23 124:1,10,12 128:2 128:3 133:21 156:20 158:19 160:16 163:1,1 174:10,12 175:1,5 213:17 215:25 216:14,17,19,23 218:8,17 221:4 225:9,13 227:15 227:16,19,25 228:15 233:2 234:1 235:13 241:25 242:7 243:2 246:3,14,20 246:23 247:9 251:18 252:4,6 256:8 260:15,17 260:22 261:16 263:9 266:18 268:4,7,9 breached 11:21 158:16 174:8 176:16,22 183:9 219:20 231:10 235:2 258:6,8 breaches 11:19 13:8 43:18 62:22 66:18 126:3 149:6</p>	<p>155:19 156:7 162:15 196:10,13 218:20 219:13 220:11,14 221:7 226:12 228:5,12 228:18 232:24 233:23 234:17 241:22 244:14 251:25 253:7,18 255:6,15,24 256:11 257:8 260:22 264:6 266:23 breadth 50:17 break 4:7 67:13 106:21,25 207:14 249:24 breakage 73:11 breaks 249:24 brief 35:22 67:22 207:16 208:14 210:5,9 briefly 8:6 54:22 223:2 248:3 256:5 bring 15:19 47:8 80:18 90:19 99:13 122:11 158:4 165:11 169:4 224:4 bringing 72:19 brings 44:11 156:17 broad 15:3 37:16 88:12 135:12 143:19 144:9 broadband 191:7 200:2 broadcast 5:4 272:11 broadened 233:14 broader 33:1 88:3 127:13 128:10 135:8 216:4 243:25 broadest 274:20 broadly 38:9,11 93:21 broke 118:5 broken 73:1,1</p>	<p>broker 53:20 brokers 172:12 brother 133:18 brothers 133:16 brought 8:11 12:7 118:20 159:10 205:1 219:25 234:10 274:17 brown 6:7 193:8 browser 120:10 browsing 57:16 Bruce 6:5 bubbles 38:2 58:15 bucket 39:2 203:11 203:12 bucketing 220:8 buckets 36:1 37:16 37:16,21 build 141:7 164:13 164:18 178:21 195:17 building 3:22 4:3,6 4:17,18,20,21,22 4:25 5:1 34:15 175:15 buildings 90:11 built 26:5 51:7 57:23 63:6 149:17 270:20 bulb 76:25 bullet 65:7 bullets 69:16 bullied 259:21 bunch 226:23 256:25 263:12 burden 131:2,5 178:7 185:2 198:20 207:2 burdened 197:2,10 burdens 198:17 bureau 1:2,3 3:14 6:22,23 14:9 20:8 59:16 134:20 143:11 208:25 209:5 215:4 270:10,12,12 bureaus 176:18 buried 166:15</p>	<p>bus 43:15 46:4 business 2:14 6:10 8:1 9:14,22 11:24 58:17 141:3 148:10,18 150:10 154:5 155:17,17 161:5 162:13 174:16,17 175:3 182:12,18,19,22 183:13 185:17 195:12,15,25 196:7,9 210:18 227:17 237:12 248:9 264:12 268:1,3 business-oriented 143:18 businesses 7:12,17 85:20 141:8,13 143:20 147:5 148:14 149:1 153:10,13,16 154:18 155:14 157:9 160:1,7,11 164:20 182:23 184:5 202:22 203:24 205:13,15 busy 53:22 button 183:10 184:1 184:10 buttons 184:21 buy 59:19 77:13 86:8 90:11 117:18 122:8 170:11 204:10 246:10 248:23 249:16,17 buying 11:15 75:6 101:25 139:10 191:15 Byzantine 117:10</p> <hr/> <p style="text-align: center;">C</p> <hr/> <p>C 2:1 3:1 19:9,13 cafeteria 4:3,5 67:14 calculate 226:1 247:20 264:19 calculated 242:16 calendar 189:7</p>
---	---	---	---	--

<p>calendars 278:16 calibrate 121:20 California 20:12 21:9,10 169:3 call 17:20 18:5 24:2 28:15 29:7,8 42:22 47:12 61:10 69:7 75:1 78:1 96:12 147:21,22 192:1 192:17,18 195:6 203:3 210:15 211:1,12 214:24 225:22 229:3,13 273:12 278:1 call-back 107:8 called 3:3 18:17 25:14 29:20,25 30:8 31:1 33:19 42:18 45:13 124:3 159:6 193:18 271:7 calling 58:11 86:19 129:8 calls 26:11 40:21 204:6 Calo's 101:3 camera 30:4,21 cancer 19:8 213:24 214:1 capabilities 182:21 capably 89:6 capacious 135:12 capture 121:1 captured 205:14 car 157:3 192:23 204:11,11,13 218:23 249:24,25 250:1 carbon 169:19 card 5:18 15:16,19 17:22,23 24:1 47:25 70:22 80:16 101:18 102:14,14 137:22 156:5 181:19,19 219:19 264:6,8,11 cards 5:14 70:14 74:16,20 76:9,10</p>	<p>102:11,18,21 129:6 141:18 146:19 255:2,5 care 53:12 77:17,18 97:13 115:14 126:3 133:24 137:8 167:5,6 177:14,16,18 178:1,2,11,19 189:6 191:9 222:1 229:5 230:10 234:19 239:5 255:20 260:9 277:21 career 142:12,25 careful 86:21 97:4 186:15 237:23 274:6 carefully 161:9 275:22 276:16 carelessly 121:18 carelessness 211:20 cares 74:18 167:8 229:6 235:11 Carl 71:1,4,8,12,14 71:15 72:21 73:8,8 75:3,6,8,14 77:2,7 77:10,13 78:12,13 78:18,22 80:7,17 82:5 85:2,4,9,10 86:5,6,12,16,23 93:5,12 99:5 101:16 103:12 119:18 120:17 Carl's 73:7 76:22,22 86:7,12 103:19 104:13 120:16 Carnegie 68:9 188:6 188:7 Carrie 6:6 carries 151:15 carry 154:17 cars 16:9 205:19,19 cascade 76:12 105:8 case 7:21 9:5 11:12 11:21 12:7 31:13 48:4 51:24 83:18 85:4,22 86:10</p>	<p>92:25 102:10 108:22 112:14 122:12 124:24 133:21 135:24 140:16 156:22 157:3 189:9 248:21 250:5 256:15 262:20 268:17 case-by-case 8:19 9:3 cases 7:9 8:12,15,16 9:5 11:7,11,17 12:14 21:9,10 30:14 40:24 45:3 56:7 80:21 97:3 98:14,15 99:3 117:20,22 122:13 127:6 198:25 200:20 205:8 208:18 212:2 225:8 226:7,8,8,11 234:15 238:11,12 248:4,4,5 250:9,9 250:10,19 263:7 cash 61:21 catastrophic 120:12 120:13 catch 120:5 167:13 188:19 189:1,21 catch-22 106:24 categories 34:4 38:21,25 39:2 130:19 156:13 categorization 83:22 categorize 79:3 category 25:1 101:2 170:21 Catherine 168:20 209:12 217:15 228:22 230:24 239:24 240:7 244:19 246:4 254:8 260:14 265:10 Catherine's 231:2 caught 30:13 43:4</p>	<p>275:5,10 causal 253:2,18 254:5,11 276:23 277:8,17 causality 120:22 250:15,17 256:6 257:11 266:23 277:12 causation 118:12 121:19 266:22 cause 37:20 38:12 125:25,25 145:15 145:16 177:8 271:25 caused 247:9 249:22 250:17 277:11 causes 34:25 35:2 49:23 60:3 67:3 167:24 254:13 causing 117:6 134:3 134:4 caution 84:21 157:22 cautious 84:18 204:16 caveat 86:15,22 CDC 39:24 CDT's 179:21 cell 170:6 Census 215:4 center 1:13,13 3:22 23:12 68:11,12 143:10 247:17 256:10 centers 29:8,8 152:8 centralized 265:6 cents 212:7 CEO 40:9 142:9 certain 19:25,25,25 55:4 57:10 58:2 79:5,6 84:10 85:3 88:25 90:15 105:17 125:25 151:18 172:4,7 204:14 210:18 219:21 221:17 225:12 226:2 240:7 241:20</p>	<p>248:9,17 261:8 certainly 22:2 38:23 49:20 57:2 74:22 77:11 93:5 111:15 136:3 139:24 148:15 153:20 170:21 186:12 216:24 242:11 247:16 253:4 261:8 CERTIFICATE 280:1 certificates 53:17 certify 280:4 cesspool 134:1 cetera 81:13 118:25 119:1,1 165:6 177:3 CFPB 59:15 Chairman 2:7 6:14 6:17 18:16 278:24 challenge 172:17 challenges 14:6,7 34:22 119:10,11 208:8 209:17 276:4 challenging 12:1 42:2 53:25 62:12 233:9 chance 39:13 91:2 114:22 225:12 227:19 change 48:16 53:21 82:25 117:14 124:4,6,6,7,21 125:2 128:7 163:6 189:24 199:18 206:23 220:24 232:13 233:7 241:12 242:5 252:18 258:23 264:25 265:5 266:13 changed 47:22 48:2 48:7 198:6 199:24 230:2 258:14 changes 69:18 126:16 163:4</p>
---	--	--	--	---

169:8 258:18 266:20 changing 43:16 185:7 250:7,8 267:1 channels 182:20 characterize 60:12 characterized 39:5 charge 8:11 258:10 charged 138:9 charges 11:20 264:10,10 chart 36:1,10,15 39:5 chatter 182:23 check 58:21 232:7 232:10 checked 58:4 232:15 checks 46:25 188:24 cheese 230:3,4,5,6,9 Chicago 108:1 142:3 chief 68:5 142:13 209:4 childhood 90:10 children 18:1 259:20 Children's 9:13 chilling 199:22 Chilson 68:5 69:11 70:8 71:8,20 74:2 76:1,4 79:16 83:6 87:1 121:6 123:5 129:5,8,11 131:24 132:21,25 133:13 135:21 137:16,22 139:11 140:20 chips 191:15,18 255:2 choice 58:15 138:12 138:23 152:5,9 167:7 170:22 171:1,18,20 183:25 184:25 185:3 187:23 197:5 201:24 204:5,9,18 choices 118:15	165:10 166:12 178:6 180:5 182:6 190:19 197:2,10 197:11,16 198:24 204:10,12,17 223:9,10,13 224:3 237:8 241:14 choose 45:18 54:5 108:14 165:17 184:11 197:19 198:4,4,8 236:17 237:10 238:11 274:10 choosing 141:13 chose 21:7 241:2 chosen 9:18 10:23 Christine 6:7 Christmas 237:4 chunk 21:3 Cindy 16:11 39:7 43:19 52:4,11 circles 22:6 circulating 61:16 circumstances 112:7 156:23 cities 185:20 Citizen 190:9 207:4 citizens 109:22 136:2 274:13 city 167:3 238:16 civil 34:15,17 36:24 56:12 claim 47:8 131:9 158:10 claims 186:2,10 220:21,23 clarify 115:20 250:18 clarity 36:24 class 24:2,4 58:4 94:3 184:20 219:22 234:16,17 234:22,24 242:6 248:21 262:19,21 263:11 classes 24:5 57:21 classic 226:21 classification 79:5	clauses 167:8 184:20 clean 60:2 228:7,9 cleanup 256:20 clear 23:23 37:2 48:6 57:21 58:16 75:25 82:7 85:12 86:4 103:13 156:1 184:1 255:25 274:8 cleared 18:14 clearing 46:13 243:9 clearly 38:5 60:25 61:2 72:2 77:5 83:17,18 85:4 114:5 123:6 173:2 237:5 271:9 clever 240:8 click 184:22 clicker 17:9 25:3 clicking 163:16 clicks 184:9 client 46:3,15 47:17 173:15 clientele 48:15 clients 16:19 45:3,10 56:7 153:22 climate 94:6 clinics 23:15 close 27:18 126:21 closed 94:1,13 closely 21:2 23:20 closer 60:1 75:1 closes 67:18 closest 141:25 closing 2:19 14:11 27:15,21 72:16 269:5 270:1,4 cloud 160:22 195:2 clueless 181:7 clustered 19:24 cluttered 198:14 CMS 24:10 co- 87:3 co-moderator 68:4 208:3 co-organizers 3:12 coalition 175:15	Coase-Sander 142:2 code 146:7 151:21 151:25 152:7,17 153:6,7 255:11 coercive 112:9 coffee 4:5 67:19 cofounder 142:21 Cognitio 142:22 cognizable 91:23 92:14 98:1 111:23 115:17 cognizant 157:10 coherence 98:4 coin 89:14 cold-hearted 78:21 collaboration 6:25 65:13,15 collaboratively 50:16 collar 214:24 colleague 194:23 colleagues 3:6,14 42:7 108:15 collect 68:20 105:4 107:15 143:21 145:25 147:12 160:12 224:16,17 224:20 234:8 247:21 collected 109:9,16 131:16 144:6 155:24 206:10 233:22 275:19 collecting 7:19 8:2 13:20 98:5,17 141:10 147:6 150:4 151:17 155:11 164:21 172:13 236:25 237:6,15 245:20 253:10 277:15 collection 10:12 33:13 59:13 81:11 82:4 83:4 95:11 96:10,24 97:23,24 98:2,22 100:10 104:22 106:1 132:16 146:16	149:2,4,8,9 151:3 155:1,9 157:6 167:21 168:6,25 169:24 172:15 184:2,9 194:8 209:7 271:23 collections 59:16 60:2 170:10 collective 36:16,19 116:22 130:3 collector 21:17 collectors 59:21,22 243:20 collects 216:6 236:18 color 187:20 Colorado 20:25 combination 42:11 combined 32:22 33:18,20 Comcast 194:7 come 5:18 26:13,14 26:15 28:8 33:10 45:10 48:11 52:2 56:8 68:17 69:2 75:24 81:5,16 88:21 91:10 104:16 106:6 110:4 112:23 124:24 134:25 141:21 169:24 179:11 196:8 205:7 208:8 218:2 219:13 221:8 246:8 247:6 254:15 comes 22:23 77:25 79:8 82:1 88:8 99:20 109:7,15 134:19 140:2 150:20 152:11 158:23 167:25 169:23 181:6 183:4 203:19 211:8 220:17 235:16 239:14 244:25 264:22 270:22
---	---	---	--	--

<p>coming 46:8 64:21 72:9,11 107:18,25 185:16 189:25 211:25 213:13 221:23 222:18 247:17 269:4 278:15,18</p> <p>comment 10:5 64:24 141:18 173:24 181:15 228:24 233:17 278:7</p> <p>comments 27:23,25 64:19 87:19 116:20 118:1 178:22 191:13 231:2 278:12</p> <p>commerce 137:2</p> <p>commercial 8:10 68:20 89:18 138:25 139:2 191:23 271:20,23 271:24 272:4,16</p> <p>commercialization 272:13</p> <p>commercially 139:10 195:21</p> <p>commingled 41:24 41:25</p> <p>Commission 1:1 3:6 3:12 143:12 270:14</p> <p>Commission's 5:7</p> <p>Commissioner 112:5</p> <p>committed 121:17</p> <p>committing 19:12</p> <p>common 41:23 95:25 226:17</p> <p>commonly 199:14</p> <p>communicates 54:11</p> <p>communicating 191:18</p> <p>communications 143:12 182:23 199:16</p> <p>communities 26:14 34:8 51:1</p>	<p>community 26:15 26:16 38:15 44:8 44:10,24 151:14 154:5 195:15 196:10</p> <p>companies 13:19 73:15 105:24 116:11,13 137:1 142:23 144:2,4 149:6,16 151:2,14 156:24 161:13,18 162:17 163:9,23 163:24 164:3,14 165:9 166:9,17,23 172:12,20 173:22 180:4 188:20,22 194:7 199:13 205:8 210:16 218:10,12 219:19 220:10,14,22 221:4 228:15 233:7 247:8,18 248:7 252:3 255:22 262:14,25</p> <p>company 17:21 53:20 56:21 64:14 64:14 70:19,24 71:3,11 78:11,15 81:17 85:1 86:11 104:8,25 105:11 110:9,10,20,24 113:6 116:17 117:1 118:22,22 118:23 150:18 153:25,25 154:9 156:9 157:14 158:18,19 160:23 161:20 164:4 169:6 174:16 183:7,8 185:8 189:19 192:8 196:15 199:2 210:17,19 213:16 213:24 221:10 224:9 225:12,24 227:17 233:2 246:23 248:9 254:2 258:6,13</p>	<p>260:1 267:25 268:3,7,14 275:16</p> <p>company's 146:9</p> <p>company-crushing 149:25</p> <p>compare 179:18 187:22 234:11</p> <p>compared 187:13</p> <p>comparison 149:5</p> <p>compassion 66:12 66:20</p> <p>compensates 56:25</p> <p>compensation 211:16 226:15,20 227:4 248:24 249:2</p> <p>competition 208:17</p> <p>complaints 20:7,9 59:14 179:22 181:11</p> <p>complement 214:17</p> <p>complementarity 240:10</p> <p>complements 239:23</p> <p>complete 30:3 134:14 173:8</p> <p>completely 24:4,5 134:6 140:6 166:6 167:10 240:25 254:10</p> <p>complex 7:2 8:24 35:10 46:21 108:16 153:4 183:23</p> <p>complexes 48:24</p> <p>complexity 152:20 182:8 183:22 184:14</p> <p>compliance 149:20 149:21,22,23,24 154:9 160:4 164:2 164:7 165:5</p> <p>compliant 147:20</p> <p>complicated 125:20 154:25 234:15 235:1 236:12 239:16 258:4</p>	<p>259:23</p> <p>complicates 260:18</p> <p>complications 272:7 276:18</p> <p>component 133:8</p> <p>components 165:14</p> <p>comprehensive 26:24</p> <p>compromised 43:10 51:18 62:13</p> <p>computer 16:2,6 30:4 41:7 110:11 185:18 210:1 245:8 251:21 252:19,21 253:21 265:2</p> <p>computer-based 66:16</p> <p>computer-related 220:23</p> <p>computers 259:18</p> <p>computing 160:22 195:2 209:21</p> <p>conceit 87:12</p> <p>concept 152:14 156:17 157:7 175:16 181:14,23 204:1,2</p> <p>concepts 159:6</p> <p>concern 82:15 104:15 167:24 169:14 198:16 199:13 261:17</p> <p>concerned 41:19 43:2 67:2 103:22 104:24 105:9,13 105:15 167:20 170:11 191:5 200:3 221:22 222:4 259:12</p> <p>concerning 41:10 42:24 155:8 162:20</p> <p>concerns 35:14 37:12 169:3 187:12 188:1 190:12,23 191:10 193:14 236:11</p>	<p>concluded 279:8</p> <p>concluding 201:11 205:25</p> <p>conclusions 69:2 230:21 254:5</p> <p>concrete 15:8 117:6 145:15 146:8 160:5</p> <p>concretely 233:10</p> <p>condition 94:17 124:17,18</p> <p>conditional 45:13 124:10</p> <p>conduct 87:11 112:8 112:9 114:19 123:22,23 124:2,5 125:2,6,25 215:19</p> <p>conducted 144:20 215:4 227:7</p> <p>conducting 215:21</p> <p>conference 1:13 4:17 278:13</p> <p>confess 211:24</p> <p>confidence 276:23 277:16</p> <p>confident 277:1,7</p> <p>confines 114:25</p> <p>confirm 116:6</p> <p>confirmation 110:15</p> <p>conflate 156:10</p> <p>conflating 35:1</p> <p>Congress 24:6 95:21 96:4,9 135:9,18 136:22 191:7</p> <p>Congressional 174:21 191:8</p> <p>conjoint 222:25 223:5,8 225:11,20 236:15</p> <p>conjunction 154:14</p> <p>connect 145:1</p> <p>connected 16:9 90:17 204:10</p> <p>connecting 252:12</p> <p>connection 187:17</p> <p>Conner 279:3</p> <p>Connor 3:13 6:23</p>
--	--	---	--	--

16:25 17:1 25:2
 32:18 39:6 43:19
 52:1 55:22 67:16
 208:4,12 211:21
 214:11 257:13
 258:17 260:12
 261:12 262:10
 263:15 265:9
 267:19 268:25
consensus 37:3
consent 31:8 72:23
 80:8 82:24 99:18
 201:25
consents 81:4
consequence 101:9
 218:7 219:1
consequences 42:3
 56:5 62:22 109:9
 154:2 218:5,16
 221:7 246:14
conservative 26:11
consider 7:24 12:10
 17:11 35:13 58:1,6
 73:14,17 104:4
 143:21 153:13,14
 153:17 160:7
 194:17 204:23
 233:1
consideration
 147:19
considerations
 141:12 150:14
considered 36:6
 37:10 73:2 134:14
 170:4
considering 58:14
 58:18 133:6
 257:18
consistent 10:14
 162:8 230:7
consistently 267:6
consortiums 159:2
constant 256:13
constantly 139:9
 185:7
constituency 62:23
constitute 85:18
 115:17

Constitution 1:13
 3:22 138:10
constrain 38:17
constraints 163:25
 200:24
construct 159:8
consultancy 142:22
consultant 208:16
Consulting 208:16
consumer 1:2 2:14
 6:10,23 7:24 8:1,3
 9:8,8,14,18,25
 10:2,15,18,23,25
 12:13,16 14:1,12
 15:24 16:24 20:7
 33:2,18 35:3,15,16
 36:4 43:23 69:19
 70:16,21 71:1,8,12
 78:17 85:10 88:8
 93:4 101:11 110:9
 110:15,18,19,24
 112:12 113:4
 116:7 118:22
 119:18 131:3
 135:14 138:23
 140:16 141:3
 142:4,7 143:22
 144:15,15 151:17
 152:4 160:3
 162:13,24 163:7
 163:16,18 165:4
 167:5 169:24
 170:16 171:18
 181:2,4,11,21
 183:12,22 184:9
 184:16 185:1,24
 186:18,23 187:23
 191:24 195:11,13
 196:17 197:1,9,12
 199:6 204:4,5
 206:9,16 208:17
 210:22 212:5,19
 219:22 221:9
 223:5 224:8 225:4
 231:22 236:3,6
 240:5 249:23
 257:15 258:16
 270:9,11,13

271:15 274:1
 275:17
consumer's 71:4,14
 85:2,9 143:7 179:3
 188:17 212:9
 236:6
consumer-facing
 149:18 163:7
 186:22
consumers 7:4,8,12
 7:17 8:20 9:1,6,9
 9:21 10:11 11:10
 11:18,20 13:7,22
 17:11 21:19 32:20
 33:15,23 35:5
 37:10 56:3 63:3,22
 70:25 73:15 80:22
 84:3 94:11 112:7,9
 120:6 131:11
 132:17 135:18
 137:2 141:9,14
 143:5,9 144:12,19
 144:25 145:7,11
 145:17,19,19
 151:5,13,15 153:3
 153:13,17 155:21
 160:3,6,8,13
 162:19,21 163:3
 164:10,18,20,21
 165:9,19 166:12
 166:16 167:5,11
 167:16 168:4,5,7
 170:5,8,8,16,20
 171:1,19 172:4
 173:4,5,19,20,22
 174:3 176:14
 177:9 179:6,11,15
 180:12,17 181:9
 181:16,25 182:1
 182:14,25 183:1
 183:17,24 184:22
 186:20 187:1,14
 188:11 190:1,11
 195:6 196:24
 197:4,9 198:21
 199:3,12,23 200:2
 200:5,25 201:5,25
 202:19,22 204:17

206:8,12,15,17,24
 211:4 212:12,24
 213:2 218:3
 222:10,12 225:1,7
 225:14 226:4
 231:5 236:11
 238:5,10 239:15
 252:10 258:1
 261:23 262:6,14
 270:17 271:13
 274:14 276:25
consumers' 7:25
 10:13 11:23 15:5
 32:21 165:25
 197:3
contact 229:17
contacts 173:14
 192:21
contained 271:17
contemplated
 147:25
content 144:11
 176:7 224:18
 267:24
contents 145:10
contest 179:10
context 10:15 13:15
 33:19 47:11 57:11
 72:19 85:23 86:22
 92:14 95:8 114:18
 119:15,16 170:1
 178:17 180:8,11
 210:11 230:2
 231:24 238:8
 239:6 241:13
 243:1
context- 119:13
contexts 34:7 35:9
 44:20 58:2 84:10
 88:7 168:1 223:7
 236:13
contextual 132:3
 140:9 176:14
 177:9
contextualized
 205:15
contingent 223:1
 226:13,21 227:6

continual 257:5
continuation 176:7
continue 11:24,25
 154:4 182:1
 259:21 271:8
 272:19 274:16
 278:5,6
continued 8:14
 99:11
continuing 71:2
continuously 120:3
contract 142:7
 258:8
contractors 139:4
contracts 142:3
 170:6
contradict 236:9
contrast 109:14
 158:5 213:1
contribution 201:22
control 40:3 63:22
 64:18 74:10 78:5
 80:12 81:19 101:5
 104:12 113:4
 138:13 143:8
 152:9 179:12
 198:22 200:4,5
 202:1 262:14
controlling 40:3
controls 132:8 265:8
conundrum 53:3
conversation 14:12
 15:8 89:2 215:20
 216:4 217:14
 233:15 271:8
conversations 34:21
 35:20 58:10
 203:10 272:3,5
conversely 224:25
convert 84:8 244:22
converting 84:19
conveyance 86:17
cookbooks 29:5
cookie 238:19,21
 239:1,3
cookies 238:15
Cooper 68:10 70:23
 71:1,6,9,12,19

<p>74:4 76:3,5 101:12 102:2 110:22 111:10 121:11 123:7 127:5 133:18 137:17,25 139:12 copious 9:14 COPPA 200:17,23 Cora 2:4 3:10 6:22 207:8 279:4 core 19:5 79:21 112:24 135:5 192:1,1 corner 49:21 164:11 cornerstones 165:3 Corp 142:18 corporate 134:2 142:23 219:18 corporations 140:4 correct 19:18 51:6 108:6 197:7 215:1 247:6 278:9 correctly 194:9 correlate 160:8,12 160:19 correlated 266:22 correlation 158:14 186:2,5,8 216:24 262:18 266:24 cost 43:14,15 73:13 107:12 119:5,20 126:12 144:11 174:11 175:1 184:7 220:14 234:1 249:16 257:19 costs 8:2 10:4,9 13:19,23 55:23 73:14,17 114:9 120:2,12,24 131:9 131:10 141:9 144:23 183:18 218:13 219:21 221:6 233:22 234:5 235:19 259:20,24 264:17 264:19,24 265:5 counsel 16:7 44:13</p>	<p>142:13 143:5 156:24 280:7,10 count 20:10,18 21:5 21:6 40:2 counter 179:5 counterparts 56:11 countervailing 85:25 88:24 107:22 118:13 counties 46:4 countless 44:20 country 136:21,21 157:21 167:3 209:11 255:3 259:3 counts 20:11,13 couple 23:21 48:20 106:13 133:1 134:9 163:13 191:13 192:9,11 200:17 219:11 220:8 coupled 262:8 course 41:1 42:21 43:6 45:22 56:23 61:21 66:18 77:4 80:9 81:21 84:22 97:1 99:17,23 100:11 101:7 128:4,6 138:10 170:2 184:3 205:19 215:23 223:22 243:6 252:7 262:13,14 272:15 court 93:22 122:19 127:14,15 223:6 235:8 courthouse 94:1,13 135:10 Courtney 6:7 courts 9:7 199:1 205:9 220:1 cousins 54:13 cover 163:2 221:14 221:17 259:19 264:13 coverage 16:20</p>	<p>262:18 263:1,7 covered 99:23 212:6 274:20 covering 48:16 221:20 covers 151:25 crawling 116:14 crazy 42:21 create 5:11 18:23 23:7 24:7 33:16 67:6 92:7 93:2 115:11 120:25 135:13 145:1 147:15 189:3 198:9 227:8 275:8 created 58:16 91:23 263:5 creates 93:14 108:4 112:10 147:8 175:25 272:6 creating 24:19 28:12 35:13 58:19 58:20 73:5 108:9 262:23 creatively 59:5 credible 197:23 credit 11:13 24:1 41:22,24,24 59:16 117:17 174:15 176:18,18 181:19 186:9,12 213:10 219:19 232:7,15 232:16 243:17 255:2,4 257:20 264:8 creditworthiness 186:3 creepy 163:4 192:20 crews 256:20 crime 16:6 18:21 19:12,24 22:8 96:6 142:23 209:8,11 214:14,16,18 215:17,18 264:15 266:6 crimes 21:4 40:11 214:20,23,24,25 215:1</p>	<p>criminal 41:25 106:17,25 249:20 249:23 275:21 crisis 20:22 22:1 crisp 242:14 crisply 58:9 criteria 12:17 critical 133:7 critically 12:15 149:20 205:3 crops 30:7 cross 129:25 244:1 cross-disciplinary 6:25 crucial 83:13 128:24 131:22 136:11,15 212:4 cryptographic 159:8 cryptologic 159:6 cued 69:25 CUJO 192:4 culling 20:6 culturally 52:22 cured 19:17 curious 71:18,20 currency 168:14 current 16:5 currently 48:4 59:3 236:22 Curtis 108:25 customer 91:23 162:3 210:17 268:14 customers 76:7 90:21 220:14 222:4 258:10 268:15 cut 255:14,15,16 cuts 105:16 cyber 16:6 32:3,10 122:9 142:23,24 143:2 149:11 209:23 219:13 220:23 221:11,16 222:3 258:18 259:1,18,21 264:15</p>	<p>cybersecurity 142:22 cycle 106:22 107:1</p> <hr/> <p style="text-align: center;">D</p> <hr/> <p>D 3:1 D.C 1:15 44:8,9 48:5 56:12 143:6 DAA 144:20 153:7 dad 166:6 Dahlman 140:10 daily 40:14 199:5 200:12 Dakota 21:21 damage 119:3 130:17 131:3 226:19 228:4 247:9 256:23 damaged 211:15,16 211:19 227:3 damages 208:20 225:24 226:1,5 228:17 damaging 25:10 119:16 138:4 Damon 25:3,4 32:18 39:11 54:2 64:6 Dan 3:15 6:21 16:25 141:6 207:8 279:5 danger 43:12 dangerous 28:8,20 137:15 dangers 65:19 dark 110:20 111:13 113:22 123:9,10 123:10 245:6 251:22,23 252:12 data 7:5,9,13,24 8:7 8:10,12,15,18 10:8 10:16,21 11:7,13 11:19 12:11,16,18 13:1,7,10,12,14 14:4 15:24 16:8,9 20:17,22 21:2,11 33:2,5,6,8,13,21 33:23 34:1,4,11,13 34:15 35:19 36:4 40:15 41:20,20</p>
--	--	--	---	--

42:10,12,14,19
 43:1 50:22 51:5,6
 51:7,11,11,15,20
 51:21,23 53:4,20
 57:12,20 58:21,21
 61:17 62:4,14 63:5
 66:18 68:18,21
 70:20,24 72:13
 75:4 76:21 80:10
 82:3,6,12 84:13
 89:15,17 90:5,6
 96:24 97:23,24,25
 98:1,2,5,17,22
 99:23 103:2,12
 104:6,22 105:1,4
 106:2 109:8,15
 110:3,15,18,19,24
 111:6,14 113:6
 114:17 116:7,12
 117:5,11 118:3
 119:18,20,23
 122:2,3,13 123:11
 123:18 126:2
 128:6,22 131:6,17
 131:18 132:16
 133:20 138:15
 139:3,8 141:14
 144:5,15 145:20
 146:1,4,9,15 147:4
 147:14 149:2,4,6,7
 149:24 150:20
 151:3,10,22,24
 152:2,4,12,20
 153:5 155:1,9,11
 155:12,19,22
 156:7,18,19,20,22
 157:1,1,6,6,7,10
 157:22,24,25
 158:1,10,15,16,17
 158:18,24 159:4
 159:13,13,14,23
 160:12,17,20,20
 161:5,7,18,20
 162:9,12,15,18,23
 162:24 163:3,9
 165:10 166:13
 167:7,12,21,21
 168:5,6,25 169:24

171:11 172:12,13
 172:15 173:11
 174:8,10,12,13,17
 174:18,23,25
 175:20,23,24
 176:2,22 178:19
 179:3 180:4,11,19
 180:21 181:14
 182:8,14 183:23
 184:1,9 185:16
 187:16,25 189:19
 190:13 193:16,18
 194:1,8 197:2,19
 198:1,23 199:9
 200:10 201:1
 202:18,20 203:5
 204:25 205:22
 207:6 209:8,16
 210:11,14,18,23
 211:3,4,6 212:2,17
 212:22,22 213:16
 213:17 215:25
 216:14,16,23
 217:24 218:8,17
 218:20,24 219:2,3
 219:5,9,13 220:8,9
 220:13,19,22
 222:17,23 224:10
 224:15,24 225:2,9
 225:13,23 226:12
 227:15,16,19,25
 228:5,12,15,16,18
 229:15,16 230:11
 231:10 232:24
 233:21,23 234:7
 234:16,19 235:1,3
 235:12 239:9
 241:15,19,22
 242:12 243:2
 244:13,20 245:20
 246:3 247:21,23
 248:10,18 251:11
 251:18,18 252:3,6
 252:15,18 253:7
 253:10,10,18
 255:6,15,16 256:7
 256:11 257:5
 260:14,21,22

261:16,25 262:9
 262:14 263:9
 264:6 266:4,18,23
 267:3,10,17 268:4
 268:7,9,14 271:18
 271:24 274:13
 275:15,16,19
 277:6,14,15
 278:14
data-driven 100:12
data-sharing 225:22
database 128:19
databases 28:23
date 25:21 158:2
 177:3
dates 214:16
David 16:1
Davis 6:6
day 4:14 14:8 41:18
 46:19 47:5,5,24
 60:6 135:14
 152:23 193:1
 197:16 208:5
 237:2 244:11
 256:12 269:3
day-to-day 60:13
De 68:10 70:14
 79:18 98:25
 101:25 110:16
 112:1 126:22,25
 127:10 128:1
 129:7 132:1
 137:19,24 138:2
deal 121:25 157:19
 194:25 197:20
 203:10,11,22
 243:19
dealing 48:4 66:9
 87:4 162:1,4
 228:18 244:4,8
 268:15 276:12
deals 248:22,24
dealt 22:3 66:20
 212:1
death 277:8
debatable 99:2,3
debate 130:15,18
 163:20 170:24

274:15
debt 21:17 59:13,16
 59:21,22,23
 243:19
decades 174:6
DECEMBER 1:9
deception 10:17
 128:10 275:17
deceptive 8:20
decide 112:22 121:2
 147:19 173:22
 206:18 224:19
 247:22
decided 70:10 185:9
 229:19 234:23
deciding 138:13
 143:21 259:11
decision 37:25 78:12
 106:11 146:4
 181:20 185:11,18
 204:13 235:1,10
 258:15
decision-making
 16:10 34:17 36:4
 36:13 37:13,19
decisional 198:17
decisions 13:21 33:3
 33:6 51:8 58:5
 73:16 107:14
 141:15 171:12
 180:13 199:6
 200:12 235:15
decode 260:23
decreases 119:22
dedicated 24:9
 151:3
deep 20:23 66:7
deeply 10:19 138:17
 166:21 230:10
default 171:22
defective 248:21
defendants 11:10
defended 116:5
Defense 143:2
Defense's 143:2
defenses 255:13
 265:8
deficient 134:18

deficits 112:10
define 35:5 58:12
 87:8 196:1 202:12
defined 35:8 57:8
 58:9 113:12
 117:24
defining 10:25 59:8
 72:2 92:16 115:13
 133:20
definitely 24:6
 187:9 199:15,19
 230:1 234:9
 261:14 274:15
definition 72:8
 73:20 87:9 119:8
 151:24 273:3
definitional 34:22
 267:22 272:21,25
degree 148:21,22
delaying 11:22
delays 257:20
delete 19:18
deleting 120:4
deliberate 230:1
delighted 168:9
deliver 181:2
delivery 181:1
delta 124:7,14 125:1
 133:17
demand 194:3
demanding 219:20
democracies 79:21
democracy 68:11
 133:8 135:3,5,25
 136:15,25 137:12
 137:15 138:5
 140:1 143:10
 184:19
democratic 138:11
 138:20
demonstrable
 123:22
demonstrate 117:1
 131:3,6,9 201:19
 242:8
denied 16:19
deniers 177:21
density 20:19

<p>deny 201:18 department 16:2 28:17 39:24 51:19 143:2 209:6 222:20 Departments 209:21 depend 163:7 184:4 268:10 dependence 140:10 dependent 119:14 depending 36:9 39:4 57:6 63:9 93:16 149:15 182:12 265:1 depends 100:21 112:22 184:19 depicted 37:18 deployed 27:25 112:6 deploying 27:22 28:6 66:4 deprivation 197:4 depth 50:17 Deputy 14:8 270:9 describe 17:12 84:8 97:16 229:24 261:6 described 7:7 95:23 108:23 196:19 describes 38:9 describing 49:16 84:1 description 210:9 226:14 descriptive 11:1 design 225:10 240:2 240:7 designed 209:18 designing 227:20 designs 58:1 desirable 228:6 desire 199:3 200:25 desires 197:3 detail 68:8 details 3:17 167:23 170:10 229:17 deter 98:6</p>	<p>determination 9:19 determine 35:4 36:6 37:9 50:23 70:13 99:16 178:13 211:2,18 240:8 determined 126:19 determining 127:16 170:17 deterring 98:22 detriment 37:17 38:14 devastating 42:3 94:19 develop 142:19 195:18 developed 130:4 165:25 214:1,17 developers 31:11,24 developing 152:22 development 195:20 developments 8:23 deviating 126:9 device 179:14 187:5 187:13 189:17 devices 3:18 63:2 179:8,12 187:8,12 189:12,22 190:24 191:15,17 192:5 192:10 205:20 devote 15:11,14 diagnoses 43:5 diagram 20:11 dialectic 72:14 dialogue 205:10 dictate 138:21 dictated 259:24 die 277:11 diets 198:6 differ 36:8 156:12 231:3 difference 64:8 100:22 113:25 129:23 186:21 250:21 differences 75:15 119:25 120:14 154:22 204:17 different 7:12 13:6</p>	<p>17:13,24,25 20:20 23:25 31:15,21 35:25 39:3 53:11 57:7,19 65:10,15 65:16 73:6 81:22 81:23 87:22 99:10 104:9 106:16 107:19 119:17 131:1,1 136:4 138:16 146:3 147:13 148:4 149:12 150:6 154:23 161:19 166:7 179:12 180:23 181:10 190:18 194:24 202:15 206:25 220:3,3,4,7,8,10 221:5 222:24 223:1,12,20,22,24 224:13 225:1,21 231:4,14 232:11 235:9 236:5 239:11 241:21 242:1 244:1,2 255:19 259:9,13 260:5,23 266:4 268:7,16 272:23 275:6,7,13 differential 35:11 159:7,8,11 differentiate 186:13 195:10 differentiator 196:15 differently 52:6 146:3 157:20 198:12 difficult 22:18 28:21 29:14 34:23 35:2 36:16 60:23 85:23 85:24 121:23 153:19 186:20 203:1 214:9 253:3 difficulties 229:2 230:22 difficulty 214:5 dig 13:24</p>	<p>digital 35:2 49:22 100:14 143:25 144:3 153:4 165:12 168:22,25 171:16 187:15 189:13 209:16 digitally 90:17 digits 238:23 dignitary 75:19 78:2 dignitary-type 79:8 dignity 109:18 130:13 dilemma 108:13 dilemmas 51:14 53:6 diligently 24:24 dimension 218:24 diminishing 201:3 direct 11:17 13:2 77:24 94:22 103:11 104:15 119:17 120:23 144:24 155:21 160:5 186:23 264:17 266:14,22 266:23 directed 195:10,11 direction 109:22 133:4 251:19 252:23 directions 107:19 251:16 directly 18:13 24:10 73:10 139:14 153:13,16 233:15 253:7 255:22 264:16,21,24 director 14:9 15:22 68:3 142:1 143:1 208:25 270:9 Disabilities 56:11 disability 16:20 disagree 164:24 disappointed 270:2 disaster 65:24 discipline 108:15 disclaimed 167:10 disclaimer 69:25</p>	<p>disclaimers 167:9 170:7 disclosed 44:3,18 45:5 48:12 49:1,12 261:20 disclosing 46:7 187:3 disclosure 10:13 43:22 44:14,15,17 45:6 56:15,19 262:24 disclosures 44:19 173:6,21 207:1 discomfort 101:7 discount 224:25 discounts 35:12 discover 270:2 discovered 270:6 discovers 110:10 discrepancy 234:10 235:22 261:13 discrete 193:2 discretion 136:19 discriminated 57:11 discrimination 16:17 38:12 42:8 45:1,2 52:14 57:9 79:10 106:9 107:7 206:11 discuss 14:5 110:2 188:16 205:5,13 260:16 discussed 18:16 32:19 60:14 81:8 152:1 154:3 186:21 258:19 271:2 276:20 discussing 15:9 16:23 69:20 discussion 10:25 12:23 14:15 17:6 38:3 66:11 69:3 80:20 119:7 125:23,23 139:6 141:8,17 143:17 207:13 222:7 269:2 discussions 7:22 8:5</p>
--	--	--	--	--

disease 19:7
 dismiss 236:10
 disparate 34:8
 display 70:13
 dispute 74:17
 disquiet 261:9
 disruption 275:9
 disruptive 275:1,8
 dissemination 209:8
 disservice 136:5
 distance 65:21
 distill 35:24
 distilled 38:5
 distinct 24:4,5,23
 156:21
 distinction 36:11,22
 75:12 77:23 79:10
 79:13 97:24
 138:25 139:5
 distinguish 231:4,16
 268:22
Distinguished
 209:12
 distress 88:15
 243:14 244:5
 distressed 244:10
 distressing 217:6,10
 244:12
 distributing 265:4
 distribution 13:13
 18:19 20:23 102:8
 108:5,12 251:4,5
 distributions 102:7
 disutility 77:24 92:5
 diverse 120:25
 197:3
 divided 101:10
Division 3:11,13
 6:10 17:2 68:3
Dixon 15:22 17:14
 49:19 54:21 59:10
 60:16 61:7 64:24
DNA 18:12
 doctor 46:11,24
 52:15,16,19
 180:21 193:19
 doctors 52:21
 218:23

doctors' 46:22
 doctrine 129:4
 documented 117:20
 117:22
 documenting 218:2
 documents 48:6
 182:16
 doing 19:21 25:13
 31:20 46:19 64:11
 68:22 105:5 131:7
 131:9 144:15
 147:20 148:2
 153:2 156:19
 158:21 161:14,25
 174:4,4 180:4
 186:14 189:19
 191:2 199:12
 202:20 203:25
 211:17 222:13
 228:12 231:21
 232:3 234:12
 237:12 239:16
 251:16 268:1,3
 275:4
DOJ 21:9
Doleac 106:19
 dollar 62:6
 dollars 19:10 32:4,7
 192:9,11
 domains 38:9
 domestic 16:12 39:7
 39:16,21 40:20
 41:14 42:16,20
 43:7 50:13 53:7,15
 62:17 64:12
 dominates 231:8
 door 43:16 48:25
 49:8
 doors 94:1,13
 135:10
 dots 252:12
 double 216:18
Doug 3:15 6:21
 208:3,12 279:4
 download 175:11
 177:22
 downloading 175:18
 downsides 51:14

downstream 33:17
 63:4 73:13 119:5
 130:15
 dox 26:11 29:6
 doxes 25:20 26:12
 26:23 27:4,9,11,18
 28:10,25 29:3,23
 59:2
 doxing 25:14,15
 60:20
 doxings 25:18,18
 26:2,4,7,8,10
 dozen 23:17
 dozens 48:14
 drains 249:10
 dramatic 108:18
 dramatically 98:6
 156:12
 draw 15:9 102:8
 155:10 254:5
 drawn 70:9
 dream 200:18
 drew 36:22
 drill 111:8
 drink 4:10
 drive 169:6,7,10,16
 169:22
 driven 185:17
 driver 46:4 277:12
 driver's 23:4 47:22
 47:25 238:25
 drivers 169:22
 driving 277:5,7
 drones 16:10
 drove 121:18
Drucker 14:3
 drug 124:18,18
 267:12
 drug-seeking 18:11
 drugs 18:7
 drugstore 75:5
 91:22 92:2 93:5
 105:4 136:6
 drugstores 105:5,6
 105:7
 drunk 277:5,6,12
 drunks 277:9
 dual-use 31:4

due 62:2 120:8
 163:24 187:7
 220:11,23 257:8
 273:22
 dumped 256:25
 duties 69:9
 duty 262:4
 dynamic 103:15
 104:1,4,16

E

E 2:1 3:1,1 4:23
 e-commerce 142:5
 144:10
 earlier 9:5 99:1
 119:6 146:13,14
 152:1,19 182:3
 226:7 237:21
 246:17 270:5
 276:14
 early 22:4 26:20
 71:17
 earning 119:22
 earth 19:16
 easier 146:18
 157:19 206:24
 246:11,24 247:3
 248:6 264:18
 easiest 234:8
 easily 29:15 73:3
 82:18 94:7 227:14
 255:7
East 4:3
 easy 24:20 35:17
 61:18,23 62:7,10
 62:20 65:19 87:15
 96:3 102:12
 121:19 147:21
 161:17 210:15
 226:7,8 246:24
 248:4,6 250:9
 eavesdrop 182:22
 echo 65:25 102:24
 104:20 153:15
 253:4
 economic 11:1
 37:17 38:11,22
 72:3,6 73:15,20,21

74:1 88:12 108:4,4
 108:24 109:17,20
 119:3,7,9,17
 130:12,20 131:3
 132:11 134:13,18
 139:19 176:1
 208:16 209:2
 211:12 226:25
 258:15 264:17
 270:15 274:25
 275:2
economically 88:3
 145:22
economics 1:3 3:15
 6:22 14:9 68:12
 107:25 108:15
 134:20 139:17
 142:2,5 208:23,25
 209:23 211:9
 245:4 270:10,12
 270:13
economist 104:11
 108:20 117:2
 121:14 134:9
 217:16,17 218:1
 230:14 239:20
 261:10 276:2
economists 73:13
 101:23 120:21
 131:22 135:1,2
 252:21
economy 131:18
ecosphere 144:7
ecosystem 49:22
 100:22 138:15
 144:3 145:14
 153:5 182:8
 211:19
ecosystems 29:22
edges 147:17
educate 154:5
 166:11 167:10
 182:1
educated 90:18
education 6:11 9:14
 38:11 165:4
 166:22
educational 165:14

<p>effect 33:20 94:19 100:23 140:10 155:25 166:24 198:15 199:22 254:15 265:16,19 effective 70:13 142:19 effectively 10:3 14:13 30:3 179:7 189:15 191:11 effects 9:24 33:17 43:25 45:8 168:23 effectuate 180:5 187:23 190:23 191:10 198:24 199:18 207:5 effort 66:1 97:17 188:7 212:11 213:11 efforts 142:19 165:8 166:10 188:14 egregious 11:8 26:10 27:3 31:10 148:12 eight 21:25 71:16 73:9 77:22 104:25 Eighty-five 144:19 Eileen 142:1 either 12:20 26:14 36:13,19 43:10 51:13 52:15 63:10 70:22 84:16 113:18 122:8,14 127:7 148:6 153:24 163:10,25 165:7 167:1 170:3 177:21 178:15,15 185:12 192:16 202:13 233:18 elderly 19:23 elected 109:23 election 38:3 elements 184:4,16 elevated 81:16 elevates 82:15 eligibility 145:23,24 146:4 Elizabeth 117:8,9</p>	<p>email 182:19 183:2 183:3,5 192:19,22 229:25 emails 242:6 emanating 96:1 embarrassed 261:24 embodied 138:10 embrace 121:9 emergency 4:16,19 4:24 18:6 28:13 emerging 20:20 214:25,25 222:3 emotional 32:5 40:2 57:1 88:14 228:4 242:2 246:21 emotionally 185:1 emphasis 212:20 emphasize 199:11 206:15 213:2 239:19 emphasizing 250:21 empirical 16:4 77:16 109:1 134:17 139:22 140:18 194:19 208:8 217:16 256:1 employed 229:23 280:7,10 employee 153:21 183:10 280:10 employer 45:14,18 71:14 73:8 107:3 120:16 136:10 employers 89:24 105:14 employment 16:17 45:1,9,14 57:9 145:24 146:5 enable 57:12 enacted 151:8,10 enacting 59:7 194:5 encompass 259:16 encountered 7:8 219:14 255:2,8 encourage 26:3 27:5 32:12 35:19 195:20 265:16</p>	<p>278:10 encouraging 31:13 31:25 39:16 212:21 encryption 159:3 195:18 218:18,22 end-all 95:6 endeavor 278:5 endeavored 35:21 ended 46:7 48:25 endlessly 202:3 ends 219:16,17 278:10 endure 47:6,10 enforce 9:11 enforced 96:8 enforcement 8:19 9:3 12:18 35:8 54:8 87:21 103:7 137:1 143:11 214:20 262:19 263:11 268:23 enforcer 8:9 11:7 enforcers 10:10 enforcing 8:16 engage 98:9 103:24 106:9 107:5 212:22 233:1 engaged 123:24 216:11 225:7 231:24,25 engaging 137:1 224:8 engender 157:7 engine 171:12 engineer 29:7 engineering 16:3 29:17 English 125:13 enhance 193:25 enjoy 63:18 168:16 169:25 enormous 109:6 119:10,11 131:13 169:18 enormously 137:3 enrolling 169:25 enrollment 23:3,3</p>	<p>ensure 12:23 22:13 57:19 58:5 66:25 ensuring 57:22 entered 19:6 entertain 74:15 enticed 30:16 entire 21:2 54:10 110:11 144:7 274:9 entirely 38:1 73:9 268:20 entirety 198:1 entities 33:7 68:20 84:2 136:1 138:25 247:22 258:8 entity 196:7 204:6 entries 19:6 entrusted 162:19 envelope 276:7 environment 47:7 132:16 146:7 152:20,21 200:22 211:10,15 226:19 227:14,15,16 environmental 169:20 208:18 211:8 213:22 226:17 228:4 environments 147:25 epidemiological 124:16 125:16 equal 149:22 276:22 equation 172:11 Equifax 113:15 116:20,25 120:20 128:21 155:21 162:17 174:11 176:21 205:7 213:6,6 246:15,18 equipped 12:21 equivalent 169:18 169:19 eroded 257:3 err 98:12 especially 3:24 8:24 29:8 36:24 38:3 52:13 54:10 66:15</p>	<p>94:10 102:13,16 114:17 115:12 130:8 139:7 149:17 151:11 155:20 163:9 167:11 172:11 177:6 182:14 189:22 199:16 201:5 228:3 233:24 241:24 255:21 271:11 espionage 142:24 essential 92:3 109:11 115:4 131:13 135:24 essentially 27:15 29:7 31:12 41:7 78:2 109:12 111:15 129:18 establish 12:17 253:3 257:11 established 126:8,14 establishments 90:16 estimate 7:15 70:21 169:10,17 estimated 113:22 estimates 169:4 234:4 estimation 250:23 251:8 et 81:13 118:25,25 119:1 165:6 177:3 ethical 58:20 203:17 ethics 16:10 37:7 203:14 EU-US 8:17 Europe 151:9 157:19 evacuation 4:19 evaluate 141:9 149:1,8 173:21 186:20 evaluated 149:19 161:8 evaluating 7:18 183:18 187:16 189:2</p>
---	---	--	--	--

<p>evaluations 162:9 event 3:12 4:13,15 5:2,5 149:25 226:16 259:20 events 4:14 62:2 250:17 eventually 46:15 252:10 everybody 91:3 117:7 143:23 175:2 235:1,4 everyday 61:9 189:7 evidence 12:4 108:23 109:1 110:21 111:14 194:15 198:5 201:17,19 256:1 evolve 9:9 11:25 148:10 evolving 9:1 154:12 166:1 196:4,5 ex 54:9 212:5,5,7,13 212:20 213:1,19 214:3 215:16,24 243:4 244:15 250:21,22,23,24 251:6,7 255:25 273:18 274:2 exact 90:6 275:12 exactly 96:25 97:19 123:16 124:23 129:18 131:19,21 138:18 193:9 214:8 234:14 252:20 256:16 258:15 273:16 examine 8:1 12:24 133:16 141:12 example 11:11,18 12:2 13:3 17:25 19:7,22 20:25 21:21 37:24 44:15 46:1,17,18 47:14 47:16 50:13 55:1,7 64:6 71:2 81:23 82:3 84:25 86:5,24 93:3 114:3,20 115:8 120:16</p>	<p>128:13 132:20,20 136:6 145:4 149:16 151:24 155:22 162:25 167:7 185:25 195:1 196:25 213:22 223:15 226:21 234:21 236:14 240:5 244:3 248:8 272:8 274:24 examples 13:4 15:8 38:19 50:19 88:3 98:22 119:12 193:2 255:1 exceedingly 120:3 exception 137:10 148:16 exceptions 218:18 exchange 33:15 99:15 182:14 238:21 excited 32:24 exciting 265:25 276:3 exclude 54:5 exclusive 38:22 executing 247:24 executive 15:22 16:11 142:16 exemplify 6:24 exemptions 218:21 261:3 exercise 57:6 96:14 110:6 165:17 175:14 182:5 exfiltrated 110:15 110:18 116:7,12 exhibit 149:3 exist 56:8 65:9 90:6 119:11 140:10,12 existed 128:21 existence 85:19 188:17 existing 38:6 57:10 exists 59:3 60:13 132:14 exit 4:22</p>	<p>expect 144:12 162:21 170:20 262:20,21 expectation 80:5 82:24 99:18 166:6 204:4 250:24 251:6 expectations 9:2,8 72:17 80:3 81:4 99:9 132:7 144:16 160:4 166:1 255:25 275:17 expected 66:13 73:13,16,16 expecting 54:12 193:19 expects 162:13 expending 9:25 expensive 19:7 59:25 170:12 273:20 274:2 experience 21:20 39:7 51:24 64:8 84:17 92:5 147:1 153:12 168:1 175:21,25 190:11 217:3,8,11 244:16 experienced 17:20 23:25 40:13 52:13 62:2 216:9,13,16 216:19,23 219:8 243:17,18 experiences 43:21 64:18 215:7,13 253:7 experiencing 40:22 266:25 experiment 240:8 268:2 experimentation 97:9,10,11 expert 14:2 22:6 64:5 149:11 194:2 expertise 139:8 278:5,7 expertises 65:15 experts 15:6 202:16 271:12</p>	<p>expiration 158:2 explain 25:10 71:24 246:2 258:22 explaining 186:7 explanation 195:4 explanations 194:18 231:5,13,16 explicitly 33:10 34:2 34:19 37:6 54:6 explore 7:14,22 70:8 128:11 141:8 exploring 10:19 15:3 exposed 82:6 92:20 113:21 213:23 214:2 251:13 exposes 110:11 exposure 55:2 93:1 expressing 241:11 expression 95:21 extended 60:4 extent 62:1 125:5 172:4,18 201:23 214:7 248:12 267:16 277:25 external 274:22 externalities 117:3 247:7 externality 118:9 121:15 212:23 extort 30:10 extra 231:8 extract 159:13 extracted 80:11 extraordinary 18:15 extremely 119:15 136:4,4 149:21,24 159:23 171:22 189:21 250:23 Exxon 226:22,22 227:4 256:18,19 256:24</p> <hr/> <p style="text-align: center;">F</p> <hr/> <p>fabulous 185:20 face 11:25 88:9,10 101:21 109:13 117:13 119:9</p>	<p>155:13 183:17 184:3 Facebook 5:4 27:18 27:22,24 28:2 54:4 54:9,12 64:19 145:3 158:24 159:12 172:7 173:10,12,16 183:4 238:15 facets 65:10 facial 22:15 facilitate 31:17 35:20 144:10 facilitating 32:1,16 39:16 facing 131:13 187:4 fact 19:20 30:16 33:2 50:22 52:2 81:12,24 83:19 84:5,11 85:8,15 100:12,17 112:20 118:24 119:4 120:8,19 125:12 126:5 138:6 160:22 165:9 166:25 167:19 169:15 177:1 184:5 185:10 200:19 212:20 248:11 250:22 264:23 268:12 factor 90:23 124:9 182:3 factors 2:11 7:24 13:9,14 68:1 160:1 160:7,10 182:4 185:6 202:24 facts 9:4 fail 34:24 149:25 failed 113:7 238:5 failing 188:14,18 189:20 failure 226:5 278:1 failures 35:7 fair 25:6 90:15,18 112:19,20 119:24 130:18 179:16 268:15</p>
---	--	--	--	--

<p>fairly 26:10 28:11 35:7 62:13 85:4 158:2 185:13 259:5 260:11 fairness 35:19 fake 22:25 28:12 229:21,22 249:21 fall 100:10 101:1 154:9 274:10 275:17 fallouts 271:23 falls 135:5 170:21 false 18:23 21:17 falsified 21:15 familiar 13:2 17:18 147:2 203:17 274:24 families 259:19 family 25:24 39:15 49:2 54:10,11 221:17 243:15 fancy 238:15 fantastic 279:1 fantasy 100:16 far 32:19 54:19 121:15,22 126:13 137:6 162:23 173:5 186:18 188:23,25 191:25 195:18 241:3 fascinating 14:15 245:8 252:13 fast 167:13 203:20 fast-changing 8:24 faster 159:1 188:21 188:23 fatalistic 127:22 fault 246:22 265:3 favorite 53:17 145:4 213:15 favorites 271:7 FBI 39:24 FCC 194:5 FCRA 36:25 fear 44:1 94:3 101:6 134:4 feasible 248:14 feature 224:6 236:7</p>	<p>features 31:5 223:12 February 278:15 federal 1:1 3:6 22:11 24:10 56:9 65:14 143:11 201:5 FedEx 181:5 feedback 9:5 240:4 feeds 134:8 feel 21:7 54:25 78:4 83:2 93:9 107:18 109:19 147:4 171:14 174:5 179:6,15 181:16 182:5,8 191:9 195:25 198:22 199:23 200:3 210:24 231:11 261:24 feeling 127:23 240:6 feels 52:18 181:4 fees 170:6 fell 222:22 fellow 3:20 136:1 143:10 144:20 felt 36:23 130:16 163:3 227:2 270:21 female 47:19,21 48:8 54:15 ferret 37:4 106:11 fertility 189:8 fewest 9:23 fictitious 19:6 field 128:24 132:6 138:20,23 265:23 266:16 267:5 fields 135:1 142:6 fight 115:25,25 116:18 142:23 fighting 116:2,15 123:4 figure 60:19 84:13 85:13 92:13 123:20 138:17 148:1 150:9 235:20 figured 42:22</p>	<p>237:23 figuring 51:3 file 19:6,14 220:25 242:5 filed 220:22 files 19:9,18 30:5 59:16 254:1 filings 11:22 fill 5:17 46:5 94:13 141:20 filter 27:23,25 38:2 120:5 filtering 27:22 64:7 64:18 filters 27:25 28:5 61:19 final 24:19 30:23 64:2,23 66:10 102:3 124:11 201:9 263:17 276:1 277:19 279:1 finally 8:3 13:16,25 16:15 46:23 48:10 59:6 73:19 77:21 82:22 92:17 110:23 221:2 278:23 finals 76:3 finance 182:15 financial 11:18 12:2 13:2 17:19,21 20:8 22:11 35:6,14 38:12 55:7,25 57:3 61:12,17 117:13 149:16 156:2 200:24 217:3,4,8 232:14 243:6 247:1 250:25 266:17 financially 280:11 find 15:16 26:6,13 31:6,21 41:22 45:21 47:9 50:15 65:7,22 75:3 98:7 106:12 115:12 116:20 117:22 130:20 132:23</p>	<p>133:19 162:7 171:8 233:3 268:6 278:11 finding 51:25 106:20 fine 47:24 79:16 112:19 127:11 170:5 fingerprint 22:15 fingerprints 239:2,7 finish 127:10 FIPPS 152:8 fire 105:14 fired 47:1 119:18 fires 71:15 73:8 78:24 firing 120:17 firm 123:24 212:16 213:4,22 214:7,9 251:10 274:4 275:19 firm's 251:11,18 firms 115:13 168:7 209:15 212:22 221:11 261:16,19 262:3 first 4:7 7:11 9:19 12:14,24 13:5 14:16 15:7 17:14 19:5 27:15,19,21 30:20 36:11,21 48:20 60:9 61:11 68:15 71:21 72:5 72:20,20 79:23 80:2 81:10 83:5 84:12 88:20 90:8 91:14 94:20 101:14 103:11,21 108:22 121:13 122:23 128:19 136:6 138:8 142:17,25 143:1 143:18 144:2 147:19 151:13 160:16 174:2 176:20 190:22 193:23 195:24 203:9 204:21</p>	<p>205:1 208:15 210:2 217:19 218:7 219:14 228:22 230:1 245:22 257:15,23 258:21 260:15 265:2 271:10,10 271:22 272:18 first-party 122:7,18 122:19 206:11 five 15:11 75:21 111:16 114:5,10 115:20,20,21 117:23 123:3 162:15 208:12 fix 24:15 57:2 60:1 196:19 250:1 fixing 55:24 flashing 176:3 178:9 flaw 270:3 flexibly 165:24 flies 152:25 flip 103:16 254:21 265:13 Florida 19:22 20:14 21:1,4 flow 96:17 271:19 flows 55:3 61:17 252:15 fluid 128:7 fly 152:23 focus 9:18 10:23,25 11:8 36:7 49:23 59:10 104:22 133:3,5 148:6 202:10,18 214:19 263:18 265:13,16 267:2 focused 16:8 209:1 217:20,21 218:2,9 218:21 220:18 focuses 9:3,24 16:13 143:6 215:17 263:18 focusing 218:24 foiled 22:18 folks 6:3 34:9,14 60:4 141:4 152:17</p>
---	---	---	--	--

152:19 164:9,24
 165:11 166:7,8
 175:9 195:25
 276:5
folks' 50:21 51:8
follow 4:17 171:17
 213:21 231:1
followed 179:25
 199:2
following 165:13
 193:10
followup 60:16
food 4:9 142:5 198:4
 267:12 275:1
footprint 157:16
forced 27:17
forcefully 134:11
foregoing 280:5
forget 137:10
form 24:3 67:9 84:7
 96:24 195:7 251:6
formally 48:7
format 143:15 202:2
formed 65:8
former 12:5 112:5
 150:18 272:10
forms 17:19 18:19
 22:2,8 23:24 24:1
 50:2 59:11 67:5
 97:12 106:16
 130:12
formula 121:2
forth 56:13 171:2
fortunate 15:5
fortunately 208:9
forum 15:23 16:8
 167:7
forums 29:24
forward 7:21 14:16
 58:24 121:24
 158:22 160:25
 234:23 235:7
 252:11 263:19
 267:21 272:22
foul 39:14
found 21:16 26:8,9
 26:24 27:9 34:21
 35:17 37:15 38:25

40:19 41:4 110:20
 165:18 194:24
 198:15 199:23
 206:4 217:9 218:5
 218:19 228:25
 230:5 245:12
founded 16:13
 40:18
founder 15:22
four 6:24 37:16
 39:25 74:24 75:17
 87:3 111:11 114:3
 114:4,10,11 123:2
 123:3 124:19
 204:12 238:23
fourth 14:5
fractions 120:6
fragmented 179:17
 200:21
framed 112:5
framework 10:14
 12:13,24 128:8,12
 129:24 145:18
frameworks 7:14
 10:18,20 58:20
 99:24 100:8
framing 71:16
frankly 87:12
fraud 24:1 35:7
 114:8 215:2
 219:21 247:2
 255:23 266:17
fraudster 11:15
fraudulent 11:20,22
 33:10 110:21,25
 114:7 119:19
 212:10 252:8
fraudulently 264:9
free 9:20 22:24 23:6
 144:9 172:5,8
 176:7 195:25
 258:10
freedom 38:17
 109:18 130:13
freedoms 51:9
freeze 213:8 257:21
freezes 257:20,20
frequent 181:19

185:13
frequently 26:25
Freund 142:8
 143:23 150:16,24
 156:4,14,16 160:9
 163:13 164:23
 174:1 175:8 181:8
 202:9
friend 40:9
friendly 198:13
friends 49:2 63:16
 71:3 76:23 77:2,12
 85:1,9,11 243:15
friends' 229:17
fringe 39:23
front 35:23 40:23
 48:25 164:19
 278:22
froze 176:17
fruits 11:9
FTC 4:12,15,24
 5:16 7:1,7,8,21 8:9
 8:19 11:6,10 13:16
 14:14 17:16 24:2,9
 34:18 35:3,8 50:12
 59:4,14 66:14 68:6
 80:21 86:24 92:12
 94:9,12 95:8 96:3
 96:13 98:16 112:5
 122:20 127:12,21
 128:11,13 129:3
 133:24 136:20
 139:15 141:19
 154:14 177:19,25
 179:10,22 200:10
 200:15,18 201:2
 201:23 202:14
 208:24 211:25
 212:1 264:4
 270:10 271:11
 273:24 278:11
FTC's 8:6 9:16
 10:17 135:5 138:5
 138:7,18 208:25
ftc.gov 5:7
fuel 193:5,13
fulfilled 162:22
full 174:7 189:3,18

266:7
function 101:23
functionality 184:6
 187:9
fundamentals 7:3
funding 276:6
funny 79:24
further 45:12 78:23
 236:2 239:18
 280:9
future 8:23 11:3
 16:7 135:13 159:1
 176:25 177:5
 187:3 205:1,10
 231:15 255:6
 273:17,21,21
fuzzier 217:24,24

G

G 3:1
GAFA 158:20,21,22
 158:23,23,24
 159:21,24 160:2
 160:21 183:3,3,5
 205:23,24
gain 29:5 211:13
gained 29:10
game 29:10 61:11
 90:19 142:5
 262:25
gamers 26:15
gaming 26:15
gamut 49:6
gap 59:7 94:13
 173:13,17
gaps 56:4
garden 49:9
Garrett 208:15
 210:8 222:13
 248:2 256:4
Garrett's 213:21
gauge 233:4
gender 34:4 43:23
 44:2,17 48:8
 152:15 155:3,6
genders 19:25
general 17:6 18:13
 61:19 76:18 157:9

163:15 165:18
 168:12 175:12
 262:13
generalizing 84:16
generally 10:19 13:2
 60:9,10 101:1
 172:6 198:16
 219:14
generated 12:9
 131:20 139:10
generation 26:22
 32:8
generator 261:5
genre 145:13
genuinely 55:15
 74:19
Geoff 83:7 89:13
 91:2,8 96:19
 102:25 103:16,17
 104:6,21 107:19
 113:8 117:20
 118:2 122:24,25
 125:10 135:22
 137:17 140:2
 273:11,22
Geoff's 87:19 94:22
 116:19
Geoffrey 68:11
geographic 19:19
geographically
 21:19
geographies 157:17
Geography 18:17
George 68:10
Georgetown 68:13
Georgia 20:14
getting 29:2,13
 55:16 69:24 77:1
 78:21 80:11
 119:24 154:25
 172:14 191:14
 196:13 219:5
 231:22 233:11
 234:17 276:14
giant 75:4
Ginger 208:22
 211:22 214:11
 215:15 230:25

231:17 234:13
 239:18 241:18
 250:12 252:24
 253:1 254:10
 261:12
girl 51:21
girls 40:6
give 6:14 35:22
 38:19 47:19 52:7
 55:5,8,14 69:25
 91:2 95:19 119:12
 159:14 170:22,25
 180:9 184:22
 185:25 201:11,25
 202:2 204:5,10
 208:14 210:6,9
 218:4 223:15
 227:12 228:5
 229:21 231:6,12
 236:14 237:21
 238:17,18,22
 239:2 251:5 252:2
 260:8 269:4
 273:22
given 9:16 35:11
 39:7 41:16,18
 42:23 43:20 80:11
 88:16 109:2
 171:19 196:18
 231:9 260:14
 261:13
gives 30:3 39:12
 190:17 225:22
giving 17:4 55:9
 202:19 204:16
 230:11 231:9
glad 174:3
Glasgow 142:15
 146:23 147:1
 153:14,18 156:6
 156:15 157:12
 160:14 170:19
 180:14,16 185:5
 195:9 196:3 203:8
 208:15 210:13
 222:16 236:4
 248:3 256:5
 262:12 267:20

glean 216:3
gleaned 18:5
global 11:12 142:13
 142:16
gloves 47:4
go 3:23 4:5 23:3
 25:12 26:6 39:11
 39:18 43:25 46:14
 46:24 47:13 50:17
 52:14 53:1,10
 54:19 57:4 59:5,24
 60:6 68:8 73:25
 82:18 86:4,8 90:22
 91:8 94:15 105:2
 106:22,25 107:14
 107:24 111:24,25
 112:4 117:10
 119:5 121:24
 125:9 128:25
 131:10 132:23
 137:25 146:21
 148:17 163:19
 164:9 174:1
 175:13 176:24
 180:15 185:9
 190:11 197:17
 201:10 210:5
 215:5,8 220:1
 234:23 239:8
 240:4 242:4,5
 245:7,9 255:18
 256:19 271:1
 272:16 273:24
 274:5 278:11
goal 7:20 69:1
goals 7:10
goes 17:11 20:19
 24:18 77:1,4 81:3
 84:11 88:18 107:8
 114:13 121:25
 124:19 133:25
 135:3 180:19
 181:3,6 185:25
 214:19 243:24
 262:20 263:6
 267:5
going 4:4 7:21 11:16
 14:14 17:3,8,22

20:4 21:20 24:12
 25:12 28:16 32:25
 33:9 42:9 46:19
 47:14,15,17,23
 49:19 50:5 51:6
 52:9 58:24 65:1,23
 66:3,5 68:19,22,23
 68:24 69:14 75:17
 78:23 85:11,11
 87:5 89:23 93:2
 94:4,4,7 98:6,7,14
 98:20 105:1,3
 106:2,5,5,22
 108:11 115:7,24
 117:19 120:10
 121:13 123:8,21
 125:12 126:11
 131:12 133:3,12
 133:16 134:24
 135:10,11 137:18
 143:16,17 146:21
 147:24 157:13
 158:25 159:22
 167:17,20 170:9
 171:13,14,23,23
 179:4,6,24,25
 181:2,5 182:6,7,24
 185:15,23 190:18
 191:20 192:11,21
 192:25 193:14,17
 195:12,23 203:25
 204:8 205:3,5
 208:14 210:4
 217:17,22,25
 222:8 223:11
 224:7,10 225:12
 227:1,1 229:2,20
 229:21 233:25
 234:24 235:8
 237:25 239:7
 240:11 242:1,19
 249:11 255:23
 256:2,6 259:21
 263:19 264:9,12
 264:12,24 265:5
 265:19 270:21
 273:13 275:5
 277:4,21 278:8,18

good 3:5 6:17 9:23
 17:17,17 34:18
 50:21 54:25 66:3,7
 102:2 106:18
 107:6 109:11,24
 118:16 143:23
 148:7 156:25
 157:5,6 162:25
 168:7,15 185:8,10
 186:6,13 191:1
 193:20 201:19
 208:2 210:24
 222:10 229:13
 241:8 245:1
 252:11 253:10
 256:9 257:10
 271:11 276:3
 277:6,14
goods 19:3 38:13
 88:9
Google 64:19 145:2
 158:24 159:12,17
 183:4 238:15
 251:20
gorgeous 65:7
gosh 230:18
gotten 45:10 125:5
 203:2
Gourley 142:21
 149:13 150:23
 158:13 174:2,21
 182:11 191:13
 204:21
govern 127:16
governed 161:12
government 9:23
 91:7,12 93:18,21
 95:17 96:14 98:11
 98:21 99:19 100:1
 100:7,25 102:5,16
 103:8 107:21
 109:2,24 113:2
 116:16 132:5
 135:24 136:9,11
 138:9,25 139:2,9
 140:3,17 147:4
 159:2 220:4
 254:23 263:22

266:9
grab 53:17
grabs 128:4
Gramm-Leach-Bl...
 9:12 162:3
grand 168:13
granular 64:17
graph 27:14
grapple 8:3 270:23
 272:1 276:5
grappling 271:14
grasp 66:3
grateful 6:1 17:16
gray 203:23
great 6:4 19:14
 32:23 39:12 63:17
 74:2,5 83:6 87:1,4
 98:18,18 112:17
 121:6 125:21
 129:5 131:24
 132:17,25 140:8
 141:16 146:17
 148:24 149:10
 150:20,20 154:17
 155:21 156:3
 164:16,17 168:16
 170:15 176:19
 183:11 190:4
 195:22 201:2
 206:5 207:10,13
 210:7 228:21
 245:8 254:19
 260:12 269:2
 270:23
greater 21:20 44:8,9
 158:19
greatest 118:5,6,7
greeting 70:13,22
 74:16,20 76:8,10
 80:16 101:18
 102:11,14,14,18
 102:20,21
ground 41:9 279:2
grounds 127:8
group 15:24 17:6
 36:19 37:23 38:8
 57:10 141:16
 143:16 151:2

208:10 251:19
grouped 37:16
grouping 37:14
groups 36:12,20
 39:3 148:5,8
 199:14,15
grow 166:4 182:24
growing 19:20,21
 193:4
grows 33:2
growth 34:16
 142:10
guarantee 116:14
guarded 162:16
guardrails 146:6,14
 152:16 203:4
guess 52:4 60:9 64:1
 75:22 121:12
 153:10 201:21
 210:8 235:11
 240:4 241:9 250:8
guidance 161:13
guide 7:21 11:3
guidelines 148:19
 161:11,12 171:15
guns 28:19
guys 129:5 133:4
 159:7,22 174:4
 205:22 222:6
 237:5
gym 47:15,18,23
gyms 47:14

H

habits 101:18
 102:14 169:16
 224:16,17
hacker 29:23 30:3
 118:5 239:9 249:9
hackers 26:16
 112:16 116:15
 249:6
half 154:1 230:2
 238:20,22 241:5,8
 241:10
Hallmark 102:19
hallway 5:15 141:19
Han 2:4 3:5,10 6:22

141:4 164:17
 166:18 170:14
 172:1 173:25
 175:6 176:11
 177:10 178:21
 179:1 180:6,15
 183:15 201:9
 202:8 203:6
 204:20 206:1
 207:10,13 279:4
hand 5:18 15:17
 32:17 53:23 69:17
 69:19 70:10,11,23
 71:1,5,13,25 74:6
 74:25 77:4 79:23
 81:20 89:19 94:4
 110:7,16,22,25
 113:10 118:18
 120:11 121:8
 123:1 141:21
 201:6 235:3,6
 252:18
handbag 193:8
handbasket 134:1
handle 176:23
 190:25 256:9
 257:6,10
handles 27:11
handling 89:10
handouts 35:22
hands 41:2 68:25
 69:4 70:4,14 71:10
 72:4 91:5 110:13
 111:3 113:17
Hansen 106:19
happen 27:3 41:21
 49:11 52:17 57:12
 66:22,23 80:12,15
 83:4 92:1 120:3,18
 121:16 170:20
 177:1,5 194:11
 212:14 227:10
 228:15 249:7
 252:10 254:13,17
 261:6 278:18
happened 18:4
 48:13 84:6 100:17
 125:7 177:4

212:15 218:18
 226:16 227:16
 228:11
happening 19:24
 20:1 21:13 22:9
 26:25 84:6 111:12
 131:19 171:10
 173:9 189:16
 227:11 232:19
 237:9 254:24
happens 18:20,21
 19:1 41:14 45:19
 45:23 46:3 54:16
 80:9 81:6 107:4
 134:20 165:10
 171:24 250:19
 261:18 273:19
happiness 211:14
happy 3:7,8 5:9
 15:12 38:19 44:5
 89:3 93:15
harass 12:6 27:6
harassing 27:23,25
harassment 12:10
 26:4 27:17 59:1
 64:9,21
hard 6:20 18:18
 24:22 32:4,6 47:8
 53:14 59:2 73:22
 74:1 83:22 93:11
 101:20 102:15
 117:22 118:15
 120:1,21 121:4,16
 122:11 123:9
 130:21 134:25
 147:21 155:16,18
 167:10 173:7
 177:5,6 178:6
 179:18,20 187:2
 189:1,13,21 190:1
 190:1,22,24
 203:20 205:23
 213:14 217:20
 219:25 226:7,11
 230:13,15 234:13
 241:15 246:15,20
 248:4 250:5,9,10
 251:17 255:23

257:11 274:18
harder 76:17,19
 86:25 159:5,5
 163:22 171:13
 185:23,24 217:23
 217:23 247:10
 249:3 261:17
harm 13:12 16:24
 17:11 19:5 20:2
 21:12 28:4,7,21,24
 32:6 36:18 37:20
 37:21,24 41:13
 43:1 47:12 48:10
 49:23,24 55:20
 57:1,7 63:8,10
 72:2,3,6 73:5,10
 73:18,20,21,21
 74:1 76:10 77:6,24
 78:2,17 79:3,8
 81:6 82:21 83:19
 85:15 86:16,19,23
 86:24 87:8,14
 88:25 89:16 90:13
 90:14,19,20,24
 91:5,19,19 92:6
 93:2 94:10 95:15
 98:1 100:5,23,23
 101:4,4,5,15
 103:11 108:18
 111:19 112:3
 114:13,13 115:17
 119:7,9,13,16,18
 120:2,18 122:15
 123:3,24 124:6,8
 124:10,12 125:1,3
 125:25 126:1
 128:12 129:19,20
 129:25 130:12,12
 130:15,20 132:11
 132:18 133:5,10
 133:20,22 134:14
 135:8 145:16,22
 196:2,4,4,6,7,8,9
 212:5,14,15,18,19
 212:21 213:2,12
 213:13,20 214:5,5
 214:6 217:13
 219:12 220:21

221:13 242:2
 244:2 248:6,14
 249:7,11,13,19,22
 250:3,19,23,25
 251:7 254:24
 255:14,20 260:5
 260:18 266:14
 268:13,13,19,21
 268:23 274:5
harmed 32:10 44:19
 56:18,22 66:6
 100:25 101:17
 115:3 258:2 268:9
 268:10,17
harmful 38:4 55:15
 118:11 156:10
 176:6
harmless 119:15
harmonization
 142:20
harms 7:4 10:7,8
 11:9 12:1 18:15
 19:4 21:18 23:22
 23:25 24:5,12,23
 24:25 27:3 28:8
 31:15,16 32:3,14
 32:16 33:9 34:24
 35:25 36:3,9,12,14
 36:16,21 37:1,3,5
 37:15 38:8,9,11,12
 38:14,16 39:2
 41:11 50:3,6,9,12
 50:14,18,20 51:12
 56:3 57:8,22 58:9
 59:11 60:3,12 62:2
 63:20 64:11 66:2,8
 66:8,22 67:2,6,7
 75:9,11,19 76:6
 78:3 81:15 83:3
 88:22,24 98:13
 120:14 127:15
 130:9 215:25
 216:9 217:4 220:5
 220:23 243:4,4
 244:16 262:2
 266:5,8 271:25
 272:12 275:18
 277:24

harp 273:13	186:11,13 190:16	276:8	276:5 278:17	hungry 195:15
harping 114:15	206:23 207:5	highly 12:8 82:14	hopeful 67:12	hurt 121:19 150:7
harvest 184:5	208:10 224:18	155:12 162:19	hopefully 271:8	170:3 174:18
hashtag 5:24	255:6 270:15,16	176:14 177:9	hoping 111:6	270:17
hat 116:3	271:8	189:8 215:2	horrible 49:4 117:6	hurting 61:15
hate 113:14 273:12	helped 64:15 66:6	HIPAA 56:16,17	174:11	hypo 69:22 70:11
hawk 237:17	134:21	hire 57:14 106:23	horrid 117:5	75:23 77:7 111:6
head 270:11	helpful 53:8 58:3	hired 62:16	horrific 40:22	111:22 115:25
headway 226:9	134:13	historical 50:25	horrifying 59:24	116:2 123:4
health 13:4 16:20	helpfully 23:5	history 57:16,17	hospital 22:23 23:2	hypothetical 10:1
21:14 44:6,16,16	helping 51:12	62:16	23:5 260:21	68:23,24 69:14,23
45:3,15 49:1 53:11	204:18	hit 121:18 183:10	hospitals 219:2,3,6	71:17 73:6 79:23
82:11,13,14,17	helpless 231:11	hits 190:20	hostage 28:14,16	90:9 94:23 96:16
139:7 152:2	240:6	hitting 264:16	59:21	96:16,22 110:4,7
185:19	helps 84:8 142:10,23	HIV 44:8 45:4,15,16	hosted 34:18	113:14 116:15,18
Health's 16:16	144:25 164:5	45:25 46:6 48:16	hostile 33:11 47:7	121:7,9 129:14
healthcare 16:18	Henderson 6:11	48:21 70:16,22	hot 21:3,20 191:14	136:10 145:4
22:9,25 23:14	hepatitis 19:9,13	71:2,3 76:9,11,14	hotels 47:14	223:11 225:15
38:10 52:13 53:1	hereto 280:11	76:22 77:10 82:5	hotline 40:21	hypothetically
53:10 56:16	Herzel 142:1	82:15,15 85:1,5,14	hours 117:9,12	152:13
hear 64:25 68:25	hesitate 49:17	86:6,8,13 93:4	house 18:9 28:12,16	hypotheticals 68:25
69:17 91:18 92:23	heuristic 96:12	94:16,16,23,24	28:18,19 34:11	83:25 87:15 93:17
179:4 242:23	hey 42:19,22 77:13	95:1 103:3,13,22	117:18 151:1	96:17 129:13,16
263:17	106:6 177:22	104:14,18 105:10	161:1,24 171:8	228:2 272:22,23
heard 25:4 33:11	hi 166:5 208:2	105:12,15 106:6	192:2 271:16	
49:4 50:4 52:3	hide 238:6	152:15 155:7	household-based	I
68:16 94:19	hiding 43:8 49:21	HIV-positive 48:15	215:3	IAPP 154:15
146:13 159:7,25	hierarchical 190:15	52:17	households 215:5,7	ID 47:25 257:19
202:15 213:5	high 21:1 36:2	HIV/AIDS 19:8	housing 38:10 41:15	258:2
219:23 220:1	120:22 124:8	hold 9:17 11:5 50:14	41:17	idea 65:13,14 79:20
221:24 236:5	162:14 186:1	255:22	Howe 6:8	80:7 81:4 82:10,22
241:20 276:8	215:9 259:5	holders 131:6	hub 211:11	87:20 89:6,8 92:6
hearing 15:13 39:18	high-definition	holding 17:16	huge 20:13 28:1	96:23 98:5 99:19
Heather 16:15 42:9	223:21	holistic 189:11	42:6 46:5 59:7	100:15 101:2,10
43:20 49:15 52:4	high-profile 30:11	holy 89:7	65:4 120:7 128:17	106:20 112:25
56:1	higher 78:18 126:13	home 43:2,9 44:23	129:2 155:9,22	120:25 123:8
heavily 149:20	213:23	53:13 117:19	186:25 187:8	127:19 128:3,17
182:10	highest 104:12,14	179:13 191:17,24	199:13,15,22	128:21 130:2
heightened 195:1,3	highlight 137:5	192:24,25 205:18	234:10 275:9	133:16 135:4
held 59:21	179:22 191:1	205:18 259:19	hugely 80:19 179:17	136:24 158:1
hell 133:25	218:8,16,25	homes 48:23 53:5	human 9:21 34:6	185:16 211:8
Hello 39:11	245:23 271:4	59:19 191:22	35:1 39:14 56:12	218:9,10 253:14
help 11:2 12:15,17	273:11 274:21	205:19	149:3	253:15
12:23 52:8 55:11	highlighted 176:13	honestly 238:7	humans 33:3 67:8	ideas 65:18 201:15
55:14 64:8,20 84:9	272:20	honor 6:13	hundred 88:14	244:14
84:10 91:14 161:2	highlighting 278:13	hope 11:2 15:7 26:3	192:9,11	identifiable 126:10
164:13 165:15,16	highlights 219:3	69:7 73:23 153:3	hundreds 30:14,14	155:2
173:21,22 186:11	272:18 275:13	189:23 206:23	30:18 31:21 258:9	identification 81:15

<p>82:2 identified 35:25 37:2 42:5 47:20 69:21 70:25 91:5 identifies 48:7 identify 7:11 50:12 51:12 62:14 85:6 92:4 95:9 98:10,13 201:23 203:21 251:24 252:3 265:17 identifying 35:6,9 37:11 42:13 44:9 51:16 67:1 83:15 98:21 121:8 126:16 155:1 208:21 216:12 identity 3:11,14 11:19 13:3 17:2,10 17:12,13,19 18:3,4 18:14,18,20,20 19:2,20 20:23 21:4 21:8,24 22:1,2,13 22:19,22 23:23,24 24:1,3,12,22,25 25:5,7 43:23 44:2 44:17 48:6 50:2,14 51:18 59:12,19 65:1 68:4 120:13 152:15 155:4,6 158:7 161:25 212:9 214:7 215:2 215:22,23 216:3 216:10,17,18,21 217:2,8 231:25 232:16 243:1,25 245:10,15,21 246:2,20 251:1 252:9 253:8,19 255:23 256:10,15 257:7 266:13 267:3 idiosyncratic 136:25 IDS 116:13 ignorant 174:5 ignore 72:8 illegal 36:23 37:2,7 37:22,22 45:22,22</p>	<p>59:13 96:11 97:22 99:25 illegally 12:3 illegitimate 43:11 79:1 illustrated 41:12 image 5:6 23:7 193:6,7,11 images 30:10 imagine 228:12 256:19 imbalances 94:12 immaturity 187:8 immeasurably 138:4 immediate 187:4 immediately 5:15 120:15,17 immense 136:19 imminence 127:3,5 127:18 immune 196:13 immutable 82:16,19 177:2 impact 32:9 36:18 38:4 50:20 62:15 100:18,23 148:17 161:21 174:14,15 174:23 175:5 243:23 255:13 276:17 impacting 26:21,25 34:17 impacts 34:8 49:24 51:1 54:18 58:19 58:22 63:4,10 imperative 97:2 implanting 255:5 implement 136:24 190:18 265:7 implemented 266:16 implicate 257:15 imply 231:13 importance 237:21 276:22 important 7:1 8:5,8 8:15,24 36:7 49:22</p>	<p>58:6,9 65:17 66:21 73:14 80:19 84:23 84:24 86:22 92:22 99:8 109:25 127:16,19 130:25 149:20,21,24 150:9,14 152:6,10 157:8,11,18,19,25 159:23 163:9,15 163:19,21 164:10 164:12 166:17 171:22 180:2 181:16,24 182:1 184:19 197:18 204:23,25 205:3 205:10,15 216:2 217:1 235:20 238:3 241:19 247:4 250:24 254:22 256:2 264:3 267:20 268:21 271:2 272:1,17 274:1 276:4,9 importantly 9:6 204:2 impose 10:9 85:14 imposing 212:24 impossibilities 116:9 impossible 66:5 128:18 256:14 imposter 18:4 impressed 66:11 117:21 impression 188:4,11 improve 34:5 183:12 202:1,1 209:16 261:25 263:22 278:5 improving 9:21 in-store 94:25 inadequate 212:25 inadequately 155:15 inadvertently 51:15 inappropriate 156:8 204:24 incentive 263:5</p>	<p>incentives 103:20 122:10 247:24 262:24 265:5 275:6,13,23 277:20,22 incidence 41:8 176:15 246:2 276:20 incident 17:20 48:12 125:3 209:24 217:7,9 243:14,17 243:19,24 246:12 246:20 incidentally 138:24 incidents 7:5,13 10:16 13:1,7 210:1 219:13,16 244:17 247:12 253:4,8 254:16 265:18 include 16:17 25:20 27:4 29:6 58:3 100:20 138:11 161:22 209:22 243:7 included 28:10 includes 25:25 38:11 72:15 including 24:10 30:4 70:25 202:4 inclusion 34:5 income 228:9 inconsistent 229:7 238:5 261:2 inconvenience 213:9 incorporate 139:16 incorporated 139:18 incorporation 139:20 incorrect 112:12 increase 73:12 85:12,20 93:12 115:16 213:2 227:8 251:11,12 256:7 257:19 270:15 277:12 increased 88:25 91:25 97:25</p>	<p>111:19 119:4 130:14,16 154:25 172:24 214:1 277:8 increases 91:20 152:3 257:11 increasing 91:24 100:11 120:5 257:7 increasingly 33:4 221:14 incredibly 25:9 42:24 60:5 73:22 106:21 119:13 120:1,21 173:7 215:5 257:13 265:25 270:19 271:11,25 272:17 incumbent 166:9 incurred 28:2,24 indefinitely 5:7 independently 92:16 indication 167:18 indicative 179:3 indignity 47:5 indirectly 244:13 individual 36:21 37:1,23,24 56:18 63:6,7 72:17 74:22 100:5,14 101:15 109:10 131:14 145:8,9 155:12 161:22 186:12 196:7 243:8,24 244:4,7 246:11,12 247:1,11,17 253:4 253:8 255:24 258:16 262:3 individual's 132:4 217:23 individualize 102:23 individualized 75:18 102:6,17 individually 38:20 221:17 individuals 12:4,6 18:25 36:14 59:13</p>
--	--	--	--	---

<p>80:22 116:23 131:15 155:23 159:20 191:3 211:4 216:16 221:10 225:21 258:11 259:6 264:16,23 industries 8:25 150:3 155:20 162:5,7,8 industry 9:6 144:1 147:23 148:7,8,12 149:14,15,21 150:2,2,10,11 151:6 154:15 157:13 158:23 161:24 163:14 165:1 166:3,8 169:1 171:15,16 171:17 175:16 179:16 180:20,23 186:6 188:24 200:10 203:5,15 220:4 233:25 254:24 263:9 273:15 275:2 inevitable 10:4 infect 29:25 infected 30:2,12 265:2 infer 61:4 inference 155:5 inferences 33:23 155:9 inferred 34:1 infidelity-promoti... 12:12 infinite 96:5 135:9 184:25 info 107:14 infoinjurfyc 5:22 inform 100:24 103:2 125:8 information 6:19 7:3,19 8:3 10:8,13 11:14,16,21 12:6,9 13:20,22,23 15:5 18:5 19:18 22:22</p>	<p>25:8,16,23,23,24 29:2,4,6,12,13,15 29:17 30:9 32:22 33:17,18,20,21,25 42:19 43:22 44:1,2 44:15,16,16 45:3 45:15 48:12 49:1 49:12 52:7 55:3,5 55:7,13,15 56:15 59:9 60:18 62:13 62:14 63:6,14 64:11 66:19 70:18 70:20 71:11 72:24 74:11 75:2 78:5,8 79:2,7 81:12 82:1 82:11,13,14,16,17 82:18 83:1 84:1,3 84:5,19,20 85:5 86:18 88:16 89:9 89:13,21 92:18 93:1,7,8,14 94:11 95:5,10,16 96:11 97:12 99:21,22 100:15 103:6,17 103:18,21,25 104:12,13,17 105:17,19,20,25 106:12 107:2,13 109:4,4,7,8 112:10 112:17 114:6,12 118:24,25 119:14 120:17 128:23 131:14,15 136:13 138:14,21 139:10 140:7,11 141:10 141:15 143:22 147:5,8,12 150:4,6 151:18 154:23 155:1,3 156:9 159:15 161:3,14 164:22 168:8,10 168:13 170:18 171:6 172:5,8 176:16 177:2 180:4 183:1,7,13 183:19 184:5 186:9,11 187:4 188:9 189:7 192:8</p>	<p>195:2 203:12,13 203:19 204:3,3 206:9 208:21 209:2,3,24 210:16 212:3,9 216:1,6,13 216:15 217:12,12 224:17,20 226:10 229:16,21 232:1 233:3,4 236:18,20 236:25 237:6,11 237:13,15,18 238:19,25 239:10 240:5 241:5,6 243:5 244:8 245:4 246:16,18 249:1,5 249:10,14,15,18 250:4,15 253:12 253:16,24 254:1,2 254:4 256:13,15 261:20 263:3 264:7 267:24 268:4,8,12,18 272:5,11,14 278:11 informational 1:6 3:7 7:2,25 8:4 9:17 9:18 11:1 14:1,6 14:12 15:10 16:23 32:21 39:8 49:18 49:20 55:24 60:12 61:9,14 65:9 75:10 156:1 168:18,19 196:25 202:12 208:9 210:4 215:24 263:19,23 267:23,23 268:11 268:16 informative 166:14 informed 140:18 164:20 166:16 201:25 informs 273:7 inherent 82:19 146:12 inherently 108:3 initial 34:10 45:11 92:9 114:25 initially 33:13</p>	<p>Initiative 142:9 initiatives 106:8 injured 10:11 79:25 85:5 86:6 88:6 92:1 96:16 197:4 245:6,16 injuries 2:9 7:15,17 8:4 9:4 10:2 12:25 13:2 14:4 15:1,7 16:23 32:19,21 39:8 43:21 49:16 49:18,21 52:2,4 55:24 66:25 83:19 84:11 87:20 107:20,22 114:5 126:12 145:15,21 146:8 156:1 160:5 176:13 177:1,8 220:5 233:22 234:2 241:20,23 255:16 264:5 271:17 276:11 injurious 152:13 155:25 injury 1:6 2:12,17 3:7 6:19 7:2,4,7,12 7:25 9:17,18,20,22 9:25 10:2,15,19,23 11:1,4 12:13,16 13:6,10,13,16 14:1 14:6,12 15:10 35:4 35:6,9,14 37:10 38:12 68:1 69:1,19 69:21 70:3,5,6 72:2,8 73:2,20 75:10 83:16,17 84:4,8,9,16,20,23 84:24 85:17,18,19 85:20,25 86:2,16 87:15,18,23 88:1,1 88:11 89:1 91:21 91:24 92:8,16,18 93:24,25 95:14 110:8 113:11,12 113:16,16,18 114:10 115:2,8,9 115:13,17 116:24 117:24 119:9</p>	<p>126:2,11,13 128:14 130:3 141:11 145:16 150:13 153:13,17 156:2 160:8,13 168:18 177:4 178:13 181:24 188:17 196:25 200:20 201:17,20 202:5,12,16,25 203:3 206:8,12 207:15 208:1,5,9 210:4,11 212:3 215:24 219:12 221:9 222:4 235:7 235:12 242:10 244:25 245:2,23 254:13 260:5,19 263:19,23 264:25 265:18,24 267:23 267:24 268:11,16 272:7 273:4,7,8,14 273:24 274:11 inkling 265:3 innocence 22:19 24:22 innocuous 28:11 62:13 74:18 innovation 9:10 97:6 153:9 209:18 innovations 97:4 input 58:2 278:10 inquisition 46:10 insecurity 88:16 insensitive 52:22 inside 4:3 5:16 141:19 insights 161:16 203:2 246:1 267:16 inspired 278:20 insta-passport 24:17 Instagram 64:19 installed 29:19 31:2 installing 22:10,12 29:18 31:22 65:2 instance 31:6 55:10</p>
---	---	--	--	--

72:13 86:12
 147:15 158:5
 181:17 259:18
instances 34:3 37:9
 52:21 200:17
instigating 278:25
Institute 10:6 142:2
 209:22 251:21
institution 9:21
institutional 51:14
institutions 12:20
 22:11
instructed 4:25
instructions 4:18
insulation 264:17
insurance 16:20
 53:11,20 56:21
 71:11 78:11,15,15
 78:18 86:11 104:8
 104:25 105:11,12
 105:24 122:7,8,20
 142:4 145:25
 169:1,6 186:2,10
 209:25 220:21,23
 220:25 221:11,16
 222:3 232:16
 246:10,10 247:16
 258:19 259:1,19
 273:15,16
insure 260:6
insured 122:19
insurer 136:10
insurers 89:24
intangibile 243:4
 252:9
intangibles 243:12
 243:21,23
integrates 9:5
intellectual 208:18
intelligence 33:25
 142:25 143:1
 193:3,12 205:2
intended 136:23
 197:8
intent 148:3
intentionally 84:19
interact 84:2 172:20
 199:5

interaction 273:6
interactions 239:24
 272:10
interacts 100:14
interbureau 6:24
interdisciplinary
 267:14
interest 15:23 70:16
 74:16 83:2 93:4
 94:23 103:12
 104:14 190:3
 199:15,19
interested 5:12
 61:10 70:18 76:22
 129:16,22 130:7
 193:9 220:2
 231:15 260:6
 278:12 280:11
interesting 60:6
 69:8 133:5 206:4
 245:11 246:8
 257:14 258:12
 259:14 266:2
 270:19 271:2,18
 274:18,21 276:4
interests 16:3,5
 99:12 109:14,16
 109:17 146:2
 209:15,22
interference 44:22
intermediaries
 32:15 173:20
 190:2
internal 131:18
 161:3 162:9 163:3
 274:22 275:15,15
 275:16
internalize 121:21
internalized 117:3
 118:9
internalizing 121:15
 149:7
international 68:12
 142:19 148:16
 154:16 157:16
 251:21
internet 16:9 25:19
 31:20 35:15 41:6

54:15 120:9 144:7
 144:9,22 145:3,8
 145:13 146:16
 176:8 191:16
 192:5
interpartner 31:16
interpretation
 230:17
interpreting 230:12
intersection 16:14
 34:15
intervene 95:17
 108:11,14 121:3,4
 131:4
intervenes 99:20
intervening 98:16
 108:13 126:15
intervention 10:3
 13:16 91:7,12
 93:19,21 100:7
 102:16 103:9
 107:21 108:8
 109:2,24 111:21
 113:2 122:21
 130:17
interventions 111:7
 242:15
interview 215:6
intimate 12:8 16:14
 31:17 40:1 272:10
intimately 94:20
intriguing 245:3
 265:23
intrinsic 78:2 82:19
 211:2,10 257:2
introduce 15:21
 68:7 113:14
 141:24 249:4
 250:6
introducing 203:13
introduction 208:14
introductions 16:21
INTRODUCTORY
 2:3 3:4
intrusion 13:5 76:18
intuitive 212:8
intuitively 89:12
invaluable 6:9

invasion 89:15
 120:15
investigate 29:13
 116:16
investigating 229:3
investing 106:3
investment 97:5
invitation 17:14
inviting 74:5
involve 11:13 12:1
 75:11 101:11
involved 13:12 33:6
 84:5 98:11 99:12
 144:2 148:18
 153:20 230:6
 234:17 247:12
involvement 138:7
involves 99:4 112:9
 223:8
involving 10:12
 11:17
iOS 159:10
IOT 179:10,10
 187:8
IP 29:9
iris 22:14
IRS 113:20
Irwin 72:12
isolated 27:17
isolating 54:10,17
isolation 32:6
ISP 25:23 29:4,8
 265:3
issue 17:22 20:19
 34:10,21 43:3 61:9
 73:25 93:11 96:22
 128:17 161:19
 166:21 169:9
 175:9 177:15
 207:2 233:11
 236:12 239:6,16
 243:2 244:4 254:5
 267:22 271:3
 273:11 278:24
issues 5:12 13:17,24
 14:10 35:10,18
 39:23 41:22 44:5
 50:1,1,3,3,4 57:24

58:13 61:14 82:9
 111:8 127:13
 139:17 148:9
 160:4 162:6
 177:12 193:21
 194:25 203:10
 208:8 210:12
 228:3 243:9 266:3
 270:23 271:14
 272:21 274:7,18
Italian 134:10
item 59:25

J

Jacqueline 3:13
 6:23 17:1 208:4
 214:14 279:3
James 68:9 71:5
 74:3 86:2,10 89:5
 111:4 113:13
 114:3 115:23
 121:10 125:11,12
 125:20 127:1
 137:16,22 139:11
 139:11
January 208:25
 267:4,4 278:8,10
Jennifer 142:15
 146:21 156:5,14
 163:22 170:18
 185:4 188:21
 192:13 195:8
 203:7 204:22
 205:19
Jennifer's 150:18
Jennings 6:5
Jersey 107:9
jiggly 176:4
Jin 208:22 211:23
 231:1 239:19
 250:20 261:13
 267:8
job 28:23 42:4 45:11
 45:21,23 46:13,16
 46:19 54:18,20
 87:4 106:18 158:9
 186:6
jobs 117:16

<p>joesknitting.com 145:5,6 join 15:12 207:10 joined 142:11 joining 14:16 143:8 143:13 joke 123:14 Jones 6:11 Josephine 209:19 233:17 236:1 241:16 246:5 248:1 253:1 254:20 256:3 258:17 263:25 Josphine 242:18 Journal 108:24 judge 12:17 234:23 241:15 judges 94:2 Juliana 6:11 July 209:1 jump 17:5,7 62:5 71:17 73:3 93:15 154:21 190:8 196:3 222:7 jumped 73:9 jurisdiction 133:25 134:6 Justice 39:24 209:6 209:6 justifiable 132:13 justify 88:24 93:18</p> <hr/> <p style="text-align: center;">K</p> <hr/> <p>Katie 143:4,5,9 148:25 154:20 156:17 162:11 170:18 172:2 176:11 177:12 178:22 180:8 186:17 188:4 198:19 206:2 Katie's 178:22 Kaufman 6:8 Kearny 142:1 keen 22:4 keep 25:16 43:23 74:16 78:13</p>	<p>103:23,25 111:7 114:15 129:8 136:12,13 156:21 163:16 205:24 248:3 264:12 keeping 163:18 kept 41:17 211:6 key 9:19 10:24 13:9 72:20 177:15 182:21 192:15 kidding 139:13 kids 18:10,14 41:16 150:25 kind 17:4 23:15 25:14 26:22 27:5 28:3,4,12,21 29:19 30:25 31:4,7 32:3 32:4,6,12,13,15,20 35:4 43:21 47:6 49:10 55:1 59:5,6 61:19 65:12 70:2,5 70:6 71:23 74:6 75:11,23 76:15,18 77:22 79:24 80:5 80:24,25 87:4,7 88:12,15 89:1,7,13 90:13 92:5 94:1,8 94:12,16,22 95:4,6 95:9,11,14,20 96:1 96:11,15 99:16 101:6 102:8,18 104:1,10 106:24 113:3,3 116:19 122:8,20,23 123:4 123:17,17,21 124:2,17,20 132:15 133:8 134:4,25 135:16 137:6 144:6,13,21 145:9,16 146:7 148:1,15 150:8 154:8,23 155:4,9 155:11 156:21 157:15 162:6 163:15,18,24 166:23 173:6,11 176:6,10,25 177:8 178:7,14 179:20</p>	<p>180:11,23 181:14 182:3 187:17,20 187:25 188:14 190:2 195:18 196:17 197:16 198:10 200:15 202:10,17,23 203:8 206:19 210:6,17 211:5,13 211:16 216:14 218:14 222:9 224:9,25 225:10 226:8 227:4 228:1 228:13,13 233:4 233:25 235:10 237:7 239:10 240:11 242:9,14 248:20,24 250:16 250:18 252:6 257:25 258:22 264:25,25 268:16 272:11 273:13,23 276:7 kinds 13:6 25:22 26:16,16 28:7,8,20 31:15,25 32:10,13 32:14,16 66:2,8 154:23 156:12 157:17 160:19 173:21 180:19 188:23 190:13 198:16 220:8 221:13,17,20 224:19 227:9 250:19 255:4 260:5 263:13 268:22,23 271:16 276:11,11 Kinko's 24:16 kit 134:13,18 knew 11:14 79:24 118:22 176:15,16 229:21 254:3 knocking 171:6 know 17:23 22:24 23:1,2,4,4 24:19 25:6,9 26:23 28:15 28:18 31:21 32:5</p>	<p>33:13,24 34:10 35:6,13 36:17,25 37:9,24 38:20,22 40:10 41:12,14 43:10,14 46:15,23 47:6,8,14 48:5,18 48:24 49:7,8,25 50:10,16 51:2,22 52:6,18,19 53:4,17 54:11 55:16,25 56:5,7,17 57:5,15 57:23,25 58:9,10 58:11,14 59:23 60:17 61:5,7,17,20 61:22 62:6,16 63:5 63:7,9,13,18,21 66:11 69:7 72:10 74:6,8,14,18 75:16 75:16 76:6,7,17,20 76:25 77:8,9,12,16 77:19,21 78:8,19 78:21,22,23 80:20 81:5,20,25 82:5,6 82:11,23 83:1,10 83:12,13,22,23 84:12 85:3 86:3,3 86:7,20 88:17 89:20 90:22 92:10 92:14 94:15,24 96:2 97:7 98:12,14 98:19 99:7,9,16,19 99:22 101:4,13,16 101:16,17,18,20 101:22 102:8,10 102:15,21 103:1,9 103:16 104:2,5,17 104:18,23,24 105:2,2,11,12,19 105:21 106:13,14 106:17,21,22 107:12 109:6 111:20,21 112:15 112:21,23 113:17 113:19,19,20 114:18,19,19,23 115:14 116:1,7,14 116:25 117:18 119:11 121:17,19</p>	<p>122:2,3,13,15,17 122:18,25 123:1,2 123:11,12,18,19 124:4,11,19,23,24 125:4,5 126:17 127:11 128:13 130:20 131:15,19 131:20,20 132:3,3 132:20 133:18 134:2,19 135:6 136:6,8,11,15,22 138:4,5 139:2,4,7 139:16 140:1,4,6,9 140:9,14 144:6,8,9 144:17,24 145:2 145:17 147:4,20 148:14 149:1,3,22 150:17,18 151:5 151:22,23 152:2 152:11,14,19,24 153:1,4,8 154:13 155:3,4,6,7,18,22 156:17,19,22,25 157:4,5,18 158:1 159:11 161:2,10 162:3 163:15,17 163:22,22 164:1,6 164:13,25 165:7 165:14,18 166:2,2 166:2,3,25 167:15 168:25 169:13 170:23 173:11 174:9 175:9,10,13 175:22 176:1,25 177:13,15,17,22 177:23 178:3,11 178:15,17,19 179:20 180:3 181:9,11,12,12,14 181:17,18,20,24 181:25 182:9,15 183:9,25 184:21 188:12 189:4,24 191:15,16,16,25 191:25 192:25 193:10 194:7,11 194:14 196:18 197:24 200:1</p>
---	--	--	--	--

<p>201:15,15,17,18 201:21 202:10,15 202:17,18,23,25 203:1,2 205:17 208:6 212:5 213:15 215:11 216:20 220:10 221:25 226:14 228:22 230:12 231:6,7 232:4,12 233:8,13,20 237:1 237:18 238:2 239:15 240:5 241:7 242:20 243:22,25 244:8 244:11 245:19 246:13 250:15,25 251:1,3,17 252:19 253:2,11,12,17,23 254:9,11,14 256:14,23 257:2,8 257:9,22 258:19 258:20,20 259:11 261:2,4,4,11,16,20 262:1,13,15 263:8 263:20 266:21,23 268:2 270:6,8,22 273:5,23 274:12 275:10 276:11,19 276:23 knowing 60:23 77:19,25 86:12 88:22,25 93:9 136:6,9 157:24 211:5,14 235:5 knowledge 17:15 92:7 206:10 known 11:15 15:24 74:12 92:19 151:16 222:25 223:5 226:13 228:6 knows 74:22,22 78:4 78:7,11,16 85:7 86:15 93:5,6,10,11 136:17 159:18 169:6 Kristal 6:5</p>	<p style="text-align: center;">L</p> <p>la 171:1 lab 190:9 207:4 240:1,8 labels 198:2,6,10 lack 122:14,14 128:23 173:7 200:3 237:13 240:5 241:5 245:1 261:9 lacking 59:1 laid 129:24 land 112:1 landscape 7:6 LANGDON 266:2 Langton 209:4 214:13 231:19 240:14 242:25 253:1 language 113:23 lanyard 4:12 laptops 218:23 large 37:15 40:12 44:12,25 48:17 51:1 57:24 60:21 66:25 124:15 161:17 169:13 198:15 214:18 215:5 234:8 244:9 256:12 265:6 large-scale 209:9 largely 38:14 167:16 168:15 201:16 larger 78:21 199:18 lasting 5:11 Lastly 5:25 276:1 late 278:20 lately 30:24 latent 89:25 launched 35:21 179:10 187:15 Lauren 16:7 32:19 39:6 law 36:24 38:6 48:5 48:9 54:7 57:10 59:3 68:12 70:2 79:11,12 87:13 89:3 93:23 95:9,20</p>	<p>95:23,24 96:10 97:5 116:4 118:6 121:20 130:4 135:11 139:6 142:1,2,3,4,4,4,5,5 142:6,7 148:3,11 162:2 166:24 167:6 186:15,19 205:6 209:23 214:20 261:15,19 262:9 263:2 lawless 138:4 laws 12:20 56:9 59:7 59:8 113:2 132:14 147:19,22,24,24 167:9 186:8 218:17 260:15,24 261:1,10 262:25 267:13 lawsuit 234:22,24 235:14 242:6 lawsuits 205:7 262:19,21 263:11 lawyer 261:10 lawyerly 93:16 lawyers 203:16 lay 261:1 Layer 88:13 layers 65:10 laziness 240:21 241:9,10 lead 28:10 31:14 38:23 84:9 86:18 123:21,24 158:2 leadership 8:13 leading 19:11 35:23 158:22,25 leads 63:3 97:17 134:11 142:10 169:10 206:11 254:16 leak 248:23 268:17 leakages 252:3 leaked 62:19 73:7 leaking 228:16 248:22 leaks 256:13 257:5 lean 112:22,24</p>	<p>LeapLab 11:12 learn 7:20 11:2 61:16 165:12 learned 267:15,17 learning 13:18 26:6 103:25 192:22 193:3,7,12 Leary 112:5 leave 3:21 4:6,14,16 4:21 60:7 69:19 140:5,19 200:8 208:24 242:19 250:9 271:4 leaving 4:22 led 163:4 left 4:22 19:13 36:15 49:9 94:2 111:5 245:17 256:22 263:16 legal 16:16 19:17 44:7,12 56:1,2 64:5 69:2 70:2 72:9 87:9,21,21 92:15 93:22 99:16 99:23 111:21 134:23 139:18,22 161:12 203:16 234:15 242:14 243:18 legally 117:25 legislation 24:7 151:8,8,10 165:23 legislators 186:4 legislature 95:21 136:20 legitimate 33:14 43:11 79:1,4 103:14 107:3 162:1 legitimately 101:19 Leigh 142:8,8,11 147:2,18 153:11 154:22 158:6 163:12 164:17 173:25 175:7 188:21 202:8 203:21 Leigh's 171:2</p>	<p>lending 278:4 Lenovo 8:16 lens 88:4 161:21 Leo 141:25 Leonard 10:5 lesser 23:25 112:2 lessons 267:15 let's 16:22 20:4 22:21 50:10,10,15 50:15,17,17 55:19 71:23 83:21 85:2,3 86:15 106:21,25 107:1 111:1 113:9 114:1 133:13 137:10 146:19 190:5 192:3 201:9 201:13 202:6 203:21 205:6 letter 48:20 263:2 letters 46:12 48:22 level 36:2,19 38:7 60:12,14 61:9,15 80:13 99:17 112:21 126:2,2,3 128:24 131:14,16 136:25 138:22 148:23 201:5 219:18 244:5 266:12 leveling 132:6 138:19 levels 100:2 210:18 levers 247:7 lexicon 17:10 LGBTQ 44:9 liability 97:18 209:25 255:3 267:12 275:24 liable 255:22 264:9 Liad 108:25 liberating 87:12 liberty 37:18 38:16 50:20 license 23:5 47:22 47:25 239:1 lie 209:15 lies 136:16 life 37:19 43:9,12</p>
--	---	--	---	---

49:24 50:5 51:24 59:20 60:13 189:7 199:5	literature 35:25 38:24 108:24 140:18	locker 47:23 48:3 locks 43:16 log 63:14 120:8 255:10	220:6,24 221:2,11 222:22 224:7 233:15 242:13 249:13 250:3 258:13 259:7,8 266:16	140:12 145:25 148:4 151:25 152:19 158:17 159:1 162:6 167:8 171:18 173:8,10 173:14 175:15 176:20 177:2 178:3 179:16 182:18 185:19 187:10 188:20 196:22 198:21 203:23 211:12 212:3,14 213:5 217:19 218:2,22 219:17,19 220:9,9 221:2,10,14 223:7 229:12 231:3 233:20 234:4,4,7 236:8 238:24 241:11,13,21 246:9 247:15 249:3,4,11 250:2 259:16 260:4,23 262:21 263:8 264:3,7 266:3
life-saving 168:23 lifetime 32:9 40:2,6 157:25 158:6 lift 62:10 64:15 lifted 257:21 lifting 257:20 light 64:15 76:25 141:10 156:7,9 likelihood 73:12 120:13 124:3,5 125:2 130:14 158:15,19 limit 271:1 limited 156:23,23 189:5 266:7 limits 8:22 112:15 112:15 275:5 line 24:15 40:23 70:9 71:24 95:15 95:15,15 101:14 102:9 159:21 162:12 177:17 178:5 210:6 230:21 linear 244:6 lines 148:1 227:21 lingered 95:1 link 77:4 120:23 121:17 123:9 212:16 252:5,7 254:12 276:23 277:2,8,17 linking 76:25 121:22 list 176:10 190:16 252:2 listen 109:22 110:1 177:20,25 listening 83:9,15 166:5 173:12 lit 77:16 literal 51:8 literally 21:16 43:8 59:19 85:19,19 91:20	litigation 94:5 little 20:15 25:7,13 32:25 36:16 37:8 39:20 45:12 47:5 52:3 53:22 55:23 68:15,19 78:1,9 81:8 86:3,20,25 92:4 130:1,2 134:7 139:19 144:17 155:18 158:14 164:1 165:15,24 180:8 183:17 193:3 195:12 196:13 210:3 211:24 218:4 219:23 222:14 233:11 238:13 255:4 271:21 273:13 274:6 live 5:4 21:20,21 61:23 88:17 122:6 210:20 225:25 226:3,5 248:8,18 lived 158:8 livelihood 50:6 155:25 lives 27:1 40:14,16 41:1,13 50:21 53:22 61:20 63:11 169:12 living 43:8 44:8 47:21 147:25 166:4,7,8 loaded 56:5 loader 120:9 loading 120:9 loads 20:7,7 loan 117:19 249:21 local 40:19 41:5 56:9 64:13 71:11 located 4:3 location 53:13 lock 213:9 lock-down 227:18 locked 174:14	logic 179:4 logical 98:3 132:13 logo 238:15,16 long 45:16 63:24 76:24 79:15 120:7 126:11 137:18 145:10 157:24,24 179:18 240:11 245:14 255:18 277:15 long-term 62:15 longer 157:2 longest 65:20,21 look 14:16 20:11 21:2 33:12 39:23 49:7 50:8,8 55:19 60:1 65:10,10 93:3 96:1 102:7,7 104:10 105:10 106:14,16 117:21 124:14,21,22 125:1,1 127:12,14 134:22,22 135:9 138:17 139:20 147:19 148:20 150:2 161:23 189:17 192:5,23 193:5,7,17 201:4 216:15 220:25 222:2 233:21 234:15 244:3,5,21 245:7 252:1 253:20 254:14 255:16 259:15 266:12,22 looked 161:20 168:24 194:6,23 222:24 262:17 looking 27:7 30:24 34:12 74:20 76:13 126:16 135:2 155:4 160:19 199:17,18 205:24 206:17 219:15	looks 261:4 268:25 276:15 loose 100:16 loosely 143:16 lose 78:5 220:11 235:8 262:14 losers 108:4,10 losing 218:23 loss 11:18 12:2 37:17,17,18 38:8 38:11,16,22,23 42:4 50:19 56:25 74:19 78:3,4 101:5 103:14 104:15 119:22 149:24 206:9 217:9 235:3 250:1 251:1,2,3 losses 103:15 217:3 217:4,5 220:24 221:1,9,13,18,21 235:25 243:6 251:4 lost 150:6 174:8 183:9 212:12 245:17 249:5 lot 17:24,25 21:9,9 22:7 24:13 25:23 26:25 29:3,4,6 31:10,14 34:3,18 45:2,3 48:25 50:21 51:11 52:12 54:22 55:12 60:3,3 61:14 61:18 63:2 65:18 66:1,15 68:16 74:7 76:16 80:20 83:12 87:19 89:11 91:1 92:23 94:5,11,18 95:19 103:4,10 105:5 110:2 121:12 133:22 138:15,19 139:16 139:20 140:9,10	lots 25:18 40:3 85:11 126:11 151:20 203:14 222:21 241:6 262:20 louder 239:20 love 174:3 263:17 loved 64:6 low 61:8,9 120:12 124:17 239:9 low-hanging 11:8 low-income 169:21 259:6 lower 60:12 61:15 78:15 107:8 169:23 lowers 71:1,12 lucky 141:16 lump 24:25 75:4 78:23 lunch 140:22,24 219:24 lying 116:17

Lynn 209:4 214:12
231:18 233:13
240:1,12 242:23
244:18 245:20
252:25 254:7

M

MAC 96:1
machine 26:6 29:20
192:22 193:3,6,12
248:22,23
Madison 12:12
234:22 235:2
magic 22:17 108:19
magical 90:3
magnitude 13:12
27:20
mail 48:24 53:5
mailing 48:14,17
main 4:21 183:21
201:21 225:6,18
mainstream 23:19
maintenance 46:20
major 176:18
228:20
majority 15:13
109:24 253:13
makers 8:22 167:6
making 9:19 48:15
51:5,8 57:19 97:22
106:10 114:13
118:15 120:21
126:12 173:3
180:12 185:18
223:10 235:15
241:14 273:10
male 47:21 48:7
males 107:10
malevolent 134:3
malintended 62:11
malpractice 88:7
malware 29:18,19
manage 14:4 200:10
managed 14:3
management 14:2
72:14 147:3
209:13,14
manager 48:2

managing 205:22
Maneesha 68:2
69:11,20
Manne 68:11 71:9
83:8 91:13,17
96:20 110:25
113:9 125:11,15
125:17 126:24
127:24 129:10
135:23
manner 4:21 131:8
manuals 152:25
manufacturer
204:13
Maps 159:17
March 187:15
mark 278:16
market 9:20 70:18
108:19 109:11
140:16 155:7
179:19 187:8
188:5 189:23
190:6 195:7
208:17 213:7
221:3,15 222:3
223:10,17 224:8
225:7,9 226:18,18
227:24,25 239:11
246:19 247:16
248:7 249:6,15
252:5,6,8 267:17
268:5 270:16
277:20,21,23
278:1
marketed 83:1
marketer 249:5
marketers 224:22
248:11 249:1
marketing 31:11
70:19,24 71:3
84:25 85:8 144:24
147:2 148:7 158:5
171:16 209:13,16
marketplace 8:23
14:14 38:13
189:24 206:18,24
271:17
markets 9:7 108:21

109:3 140:12
193:25 271:12,13
Maryland 56:12
208:23
Mason 68:10
material 31:12
materialized 130:17
materials 5:11
math 22:16 229:12
matter 11:2 13:10
19:1 48:6 70:4
80:3 114:4,11
137:6 163:20
194:15
matters 9:20 78:10
132:5 180:11
200:16 236:9
Maureen 6:14
maximizing 158:3
maximum 142:20
McCoy 16:1 25:12
58:25 60:25 65:25
McInnis 143:4
149:1 154:21
155:16 162:12
172:3 176:12
178:24 179:2
186:18 188:18
190:8 198:20
200:15 206:3
mean 47:7 49:6 50:7
56:25 57:1 60:21
62:20 74:17,19
75:10 76:15,18
78:10,13 79:4 87:8
88:19 89:19 91:22
92:15 93:17 94:24
97:10,11 101:19
101:20 103:3,4,7
103:11 104:4,10
104:11 105:2,18
106:4 107:8
111:13 118:11
121:14,14,16,22
122:5,6 123:4
124:2 126:1
127:14 128:23
136:23 137:8,9

139:6 163:14
166:13 167:16
168:10,17 175:3
178:20 180:20
181:3 183:23
190:2 191:4
197:24 212:18
225:10 239:15
241:17 244:5
245:2 251:9 253:9
253:23 261:25
263:4 267:23
271:5
meaning 106:21
meaningful 49:24
50:9 106:23
159:15 178:14
198:7
meaningfully 54:24
meaningless 81:24
81:25
means 40:8 43:11
47:20 79:11 81:14
82:12,25 89:25
98:15 133:21
167:21 171:21
174:7 216:2
217:16 247:21
270:11
meant 60:17 218:22
measure 8:4 14:5
28:22,24 66:2
134:25 210:11
212:4,10 214:7
217:20 220:7
222:9,11 225:4,20
227:4 230:15
233:9 235:20
238:7 242:21
245:21 247:3
248:6 249:13,19
250:7,16 251:12
251:13 254:11
258:1 259:9
263:23 265:15,21
266:4,8,9,10,11
267:6 268:24
276:16,17

measured 14:3
169:16 250:3
measurement 16:4
246:5 258:23
276:9
measurements 66:4
66:7
measures 22:12
195:3 209:10
214:15 262:7
measuring 2:17
7:15 207:14 208:1
208:5 210:4 214:5
214:5,6 222:17,17
226:9 228:17
231:20 236:3
244:20,25 245:22
248:13,13
mechanical 152:24
mechanism 59:24
mechanisms 12:19
117:4 255:19
media 5:8 54:4
261:23 262:18
263:1,3,10
mediated 272:4
275:20
mediating 140:16
medical 18:2,14,18
18:19,20,23 19:2,6
19:14,18,20 20:23
21:3,8 22:1 23:23
24:12 25:4,22
40:15 43:3,5,6,22
44:1,7 46:5 50:2
50:14 52:24 56:15
56:20 59:11,13,19
60:1 65:1 88:7
94:17 120:13
168:22 180:22
193:16,18 219:5,9
medical- 44:6
medication 46:25
48:21
medications 48:16
meet 206:5 261:19
263:2
meeting 122:15

193:19
Mellon 68:9 188:6,7
member 164:2
 165:8 234:24
 235:5
members 3:20 49:2
 156:25 165:2
 199:14
memories 90:10
men 40:5
mention 71:8
 127:20 206:7
 277:19
mentioned 11:6
 33:16 37:21
 101:17 118:19
 128:16 147:18
 151:21 152:19
 163:22 184:17
 188:22 193:24
 200:24 205:19
 214:14 226:7
 236:15 237:21
 243:13
message 120:4
messages 154:17
met 17:25 116:5
method 29:7 81:25
 223:6
methodically 67:1
methods 57:19
 210:21
metric 109:24 121:1
metrics 209:24
Michelle 68:10
 79:17 87:16 89:6
 95:6,22 98:24
 102:25 103:4
 111:25 122:1
 129:17,19 130:8
 131:25 133:8
Michigan 166:4
microchips 255:5
microphone 30:4
middle 23:7
middle-income
 259:8
midmorning 4:7

midway 88:21
milk 275:3
million 20:18 62:6
 78:25 113:21,22
 174:12
millions 258:9
mind 3:24 69:18
 79:13 95:14
 135:19,25 136:4
 163:16,19,24
 164:19 262:2
 272:20
mine 278:6
minimization 157:1
 157:8,10,23
 175:23
minimize 263:1
minor 62:14
minute 64:1 75:13
 91:18 201:11
minutes 15:14 80:15
 111:5 192:24
 200:8 263:16
mired 34:22
misappropriation
 274:23
miscreant 62:3
miscreants 39:19
misdemeanor 96:5
mishaps 200:10
mishear 134:16
mismatch 236:5
 237:16 238:4
 239:13
misnomer 30:25
misogyny 54:16
missed 75:25
missing 214:21
mission 135:6 153:2
 270:12,13 271:12
 271:13
mistreating 268:14
mistress 102:1
misuse 7:24 10:8
 11:16 15:4 162:23
 208:20 210:14,16
 211:3 212:21,22
 216:1,12 232:1

243:5 244:8
 274:22 275:15
misused 40:25 52:9
 123:19 163:2
 217:12
misuses 212:8
MIT 229:9,19
 230:18 239:25
MIT's 209:14
Mithal 68:2,2 69:24
 71:5 91:1,16 96:19
 98:23 107:17
 110:2 111:24
 113:8 115:22
 125:10,14,16
mitigate 34:6 51:4
 64:9 148:21 242:3
 273:17,21 274:2
 277:23,24
mitigated 28:4
 67:10
mitigates 202:20
mitigating 37:11
mitigation 36:8 39:4
 51:12 156:11
mix 66:12
mobile 3:18 31:2
 188:8
model 144:22
 150:10 198:8
 245:1
models 11:24
 185:17 187:22
 203:14 209:25
moderately 217:10
moderating 69:9
 141:7
moderators 115:24
 273:4
mom 18:10 166:5
moment 39:10
 113:6 114:2
 131:12 230:9
 260:10 261:21
monetize 272:13
monetized 272:6
money 24:13 30:11
 56:24 168:8,10

178:6 190:17
 212:11 213:12
 229:12 232:18
 260:4,7 274:5
monitor 12:15 41:6
 58:20
monitored 27:12
monitoring 117:11
 232:17 251:23
month 194:9 249:8
 249:11
monthly 223:22
months 18:12
 120:19 216:14
 244:7 257:9
Mooy 68:10 70:14
 79:18 98:25
 101:25 110:16
 112:1 126:22,25
 127:10 128:1
 129:7 132:1
 137:19,24 138:2
morning 3:5 6:17
 147:10 154:3
 241:21
morning's 141:8
 153:24
morph 23:6,8
morphed 23:12,16
morphing 24:14
mortgage 64:14
 182:15,16
mosaic 33:19
motivated 66:23
motivates 274:4
motive 275:3
move 20:3 43:13
 59:20 61:24 64:15
 89:3 110:3 132:10
 148:8 171:11
 195:23 201:9
 232:12 235:7
 240:16,20 242:20
moved 137:23
movers 43:16
moves 35:15 124:11
movie 237:8
movies 236:19,19

moving 55:23
 101:13 139:21
 159:1,20 167:12
 188:21,22 255:21
muddy 271:21
multifactor 255:9
multifactorial 65:11
multiple 4:13
 231:10
multiplied 33:5
multitude 260:17
must-do 170:23
mutually 38:22
mythical 96:14

N

N 2:1,1 3:1
NAI 142:11 147:3
 148:5 175:13
naive 116:9,17
name 3:10 17:1
 42:15 48:1 68:2
 69:6 89:21 124:25
 146:19 208:2
 234:25
named 85:10
names 25:20 251:24
narratives 59:17
narrow 114:25
 119:8
narrow-minded
 212:14
narrowing 58:15
narrowly 73:20
 135:3
narrowness 225:6
nasty 198:10
Nathan 6:9
national 16:12
 209:8 214:14
 215:17 240:3
 260:18 266:6
nationwide 40:21
natural 222:21
 265:14,20
nature 215:13 267:1
naval 142:25
navigate 35:18

<p>Navy 174:20 NCVS 215:3 253:17 266:6 near 80:16 nearby 46:4 necessarily 53:8 61:15 66:13 76:24 77:18 113:2 119:2 128:20 151:16 152:24 162:25 166:14 176:9 191:4 197:21 239:12,15 242:1 247:23 259:17 necessary 45:6 148:10 necessitate 107:21 need 3:16 8:22 10:2 10:10,14 12:24 13:9 14:4 15:16 41:22 46:14 48:8 53:19 57:18 84:18 117:3 134:21,22 137:14 147:18 151:4,5,7 154:11 154:11 155:10 156:7,8,18,21 157:1,2,24 161:8 171:4 174:5 175:24 191:21 197:17 205:14,16 205:24 212:23 218:10 219:6 224:25 226:16 230:19 252:7 254:18 256:8 257:6 262:15 270:23 272:1 273:9 274:6 275:22 276:5,11 276:15,17,19,22 277:15,20 needed 271:9 needing 241:18 needs 24:6 41:19 52:24 55:12 139:15,18 158:16 161:20 201:24</p>	<p>203:3 272:19 273:15 274:16 negative 7:22 12:21 15:3 45:8 58:22 212:23 257:1 negligence 62:3 88:10 205:9 neighbor 40:9 neighborhood 213:23 neighbors 49:2 Neil 68:5 69:8,10 83:8 neither 168:11 280:7 NERA 208:16 210:25 222:18 262:18 net 16:13 40:17 86:1 86:9,18 200:1 259:5 NetDiligence 220:22 Netflix 237:1,2 network 16:12 58:15 71:4 76:23 77:12 85:2,10 86:12 110:11 116:3 142:9 179:20 264:11 networking 25:25 27:4,10 28:5 networks 116:5 219:20 neutrality 200:1 Nevada 20:25 never 8:8 57:4 96:8 98:7 116:10 155:23 160:24 224:15 226:25 236:17 237:10,18 238:1 new 9:9 12:15 17:22 20:15 25:5 35:14 50:12 58:24 94:25 95:12,12 96:23,23 97:11,12 107:9,9 148:9,9,9 154:13 154:14 165:24</p>	<p>168:8 183:11,11 187:5,5,19 190:10 238:16 264:1 278:13 newer 32:8 97:3 news 12:10 48:13 241:8,9 nice 28:3 67:11 166:22 nicely 10:6 niche 60:2 Nicole 6:11 nine 73:4 77:22 104:25 nodding 219:7 nonconsensual 59:9 nonpersonal 155:1 nonpersonalized 178:9 nonprofit 188:7 nonvictims 216:11 nonzero 114:21 Nordstrom 152:12 181:19 normal 121:18 149:3 192:6 normalize 20:17 21:11 normally 25:20 29:19 norms 58:12,16 72:17 North 21:21 Norton 192:1,3 note 39:20 51:10 67:12 noted 271:22 notes 49:9 nothing's 106:2 notice 4:25 29:3 113:4 152:5,9 noticeable 113:25 noticed 194:6 270:3 notices 171:4 notification 53:12 53:24 218:17 260:15,22 261:15 261:18 262:4,9</p>	<p>notify 53:19 noting 10:6 notion 74:15 118:12 133:7 NSA 114:24 NTIA 199:22 nuanced 120:25 nuances 65:23 120:1 number 27:9,20 33:3,5,7,16 34:9 55:9,10 73:23 74:24 75:21 76:20 77:5 84:14,25 91:11 93:3 95:17 97:15 111:10,16 112:1 113:1 114:3 114:4,5,10,10,11 116:16 118:18 123:1,3,3 155:19 162:14 172:11 174:19,22 175:4 181:13,18 189:22 191:3 192:20 212:1 215:19,22 219:22 229:19 238:24 249:16 255:15 numbers 25:22 28:9 39:24 40:8 41:10 104:25 216:20 220:18,24 245:17 255:7 numerous 142:18 166:25 nutrition 198:2,6 NYU 16:2</p> <hr/> <p style="text-align: center;">O</p> <hr/> <p>O 2:1 3:1 objectionable 83:21 objective 101:4,8 obligations 8:10,16 81:17 99:22 154:9 261:19 observation 104:3,3 194:22 observe 212:17 obstacle 183:21</p>	<p>obstacles 183:17 186:18,25 obtain 211:4 257:20 obtained 12:3 253:13,16,24,25 254:1 obvious 11:9 13:11 41:12 242:7 243:7 obviously 41:19 74:18 86:14,16 92:14 113:12 156:19 163:18 185:18 224:6 242:3 252:11 266:14 occasions 265:17,25 occur 9:10 12:25 32:20 37:4 38:9 120:14 271:17 occurred 70:7 80:2 80:13 87:11,23 110:12,14,17 114:20 116:6,8,21 119:3 120:15 155:20 200:20 241:25 occurrence 7:16 occurring 22:9 32:14 47:12 81:3 83:4 277:24 occurs 4:16,19 45:20 132:19 oddly 46:9 odds 123:18,21 124:7,12 offenders 40:25 offer 9:14 45:13,22 45:24 118:7 187:8 224:14,25 230:3,9 258:14 offered 33:14 100:25 258:10 offering 194:7 221:11 273:17 office 6:12 61:10 143:6 officer 143:1 153:25 offline 54:17</p>
---	--	--	---	--

<p>offset 128:15 oftentimes 26:2,18 26:19 30:7,25 32:3 32:7 61:6 265:23 oh 17:21 20:4 21:8 22:24 53:19 65:1 67:16 77:1 78:22 111:24 121:3 129:7 137:24 150:16 156:4 173:14 178:18,22 194:15 229:1 230:17 235:11 254:9 Ohlhausen 2:7 6:14 6:17 18:16 Ohm 68:13 70:14 87:3 93:15 110:13 115:24 132:23 133:11,14,19 oil 226:23 256:19,20 256:23,24,25 okay 15:2 20:5 46:11 49:4,14 55:13 60:5,19 62:1 64:22 67:11 75:2 76:21 91:4 93:14 95:17 96:20 98:23 103:12,17 108:3 110:2,8,14,16,19 111:1,10,25 112:1 115:22 116:17 123:3 126:22 137:24 139:12 141:6 143:15 147:1 148:24 150:13 153:10 154:19 156:3 158:12 159:25 163:11 164:16 178:21,25 190:4 195:22 196:23 198:18 200:7 201:7,9 204:21 232:8 235:2 236:1 237:5 241:4 242:18 251:6,22 260:3,12 261:18</p>	<p> 262:4 263:15 278:9 old 14:2 20:1 48:1,1 48:1 older 90:17,22 215:6 Olivia 6:7 Omri 141:25 142:8 166:19 177:10 180:7 183:20 188:2 193:23,23 201:13 221:24 Omri's 178:22 198:20 once 69:17 184:15 250:6 one's 38:14,17 194:1 one-third 239:1 onerous 151:23 164:8 ones 13:11 26:9 37:6 60:22 62:8 72:4 118:19,20 148:17 153:20 184:19 223:14 226:11 247:23 ongoing 9:7 14:12 274:15 online 5:11 8:13 9:13 25:21,25 28:5 29:5 57:16 59:1,9 63:1,15 64:8,20 144:6,8,24 145:10 146:2 155:5 171:1 172:12 175:25 190:13,16,25 191:6 199:12,16 199:20,22,23,24 207:6 onus 173:18 opaque 36:14 open 4:6,9 67:14,16 67:18 133:4 135:10 228:21 249:20 opened 260:14 opening 2:6 6:14,16 72:15 openly 129:13</p>	<p>operationalizable 126:7 operations 209:16 operator 12:7 opinion 99:24 204:18 261:1 opinions 202:16 OPM 174:10 176:15 opportunities 147:7 161:8 opportunity 37:17 38:8,23 39:18 119:20 154:4 161:15 171:24 261:7 273:17 opposed 54:24 125:3 198:13 203:20 259:25 opposite 96:25 120:11 263:24 opt 54:1,4 55:4,6 192:7 opt-in 186:24 opt-ins 198:24 opt-out 175:14 opt-outs 61:18 186:24 198:25 opted 155:23 optimal 109:3 126:2 126:2,3,9,20 optimally 108:22 optimistic 127:24 option 224:20 options 165:16 193:25 194:10 order 3:3 55:2 111:2 172:8 176:4 203:3 213:10 239:1 ordered 181:5 ordering 28:11 253:2 254:5 orderly 4:21 orders 42:17 ordinary 229:17 organization 34:20 143:3 171:2 176:15 186:22,22 organization's</p>	<p> 142:10 165:8 organizations 40:20 40:24 172:20 177:7 organized 18:21,22 143:16 organizers 199:17 organizing 207:8 orgs 153:7 orientation 43:22 44:2,17 oriented 195:21 original 23:11,12 53:13 originally 142:17 Orion 142:18 Otlewski 6:10 ought 95:17 ourself-regulatory 165:3 outcome 12:22 78:6 105:13 246:25 248:13,14 266:17 273:18,21,22 274:3 277:4 280:12 outcomes 7:23 15:4 68:16,17 109:11 240:16 242:21 244:2,20 246:8,11 247:11 248:5 252:10 266:21,25 267:1 276:12,18 276:20,25 277:3 277:18 outlaw 59:3 outlier 199:14 outreach 165:4 outside 4:2 5:15 15:17 53:1 95:8 162:10 275:20 outsourced 181:1 outwardly 47:21 over-the-counter 70:16 overall 37:13 38:5 124:20,22 125:3 overcome 209:3</p>	<p>overdeterrence 97:8 overdetering 97:5 overenforcement 97:8 overenforcing 97:5 overestimate 149:4 overlooking 206:13 overly 93:16 overnight 256:22 overpolicing 51:13 override 169:14 oversee 214:14 overseeing 209:7 overuse 212:21 overview 228:20 owe 226:4 227:5 248:23 249:2 owed 211:16 226:20 owners 256:22 ownership 252:16</p> <hr/> <p style="text-align: center;">P</p> <hr/> <p>P 3:1 p.m 140:24 141:2 279:7 PA 4:18 package 181:5 224:18 packages 194:8,8 packet 38:18 68:8 page 2:3,6,9,11,14 2:17,19 120:8,9 176:4 206:6 241:3 pages 61:2 paid 31:24 64:14 206:13 248:16 painful 83:20 painkiller 18:7 painting 7:6 139:1 Pam 17:8 25:2 Pamela 15:22 64:3 65:25 panacea 82:8 157:23 panel 2:9,11,14,17 3:25 13:5,17,24 14:5,17 15:1,6,13 16:22 17:3 32:25</p>
---	---	--	--	---

<p>44:11 60:10,10,11 60:14 66:14 67:13 67:13 68:1,14,16 68:18 72:10 79:12 81:8 85:24 88:20 94:20 130:7,16,25 131:2 133:6 134:24 141:3,7,12 143:15,24 153:24 202:17 205:5,12 206:4 207:9,14 208:1,3,4 212:6 219:24,25 221:24 250:20 251:10 267:9,9 271:10,22 272:18,20 274:9 274:17 276:1 panelist 17:4 210:2 panelists 5:25 15:12 15:21 16:24 17:6 33:12 49:15 64:2 68:7,24 69:5,12,15 87:3 92:23 121:7 140:21 141:16,24 143:13 153:12 164:25 180:9 196:1 200:9 207:11 208:10,13 213:5 228:22 234:9 260:16 269:2 272:22 276:19 278:3 panels 5:14 15:9 146:14 147:10 152:1,20 167:3 208:7 270:19 271:4 274:19 276:14 panicked 196:21 paper 224:11 252:2 paradox 229:4 231:2 paralegal 6:6 15:19 paralegals 15:18 parentheses 198:5 parents 166:4 part 4:7 6:1 10:24 17:10 27:10,15,22</p>	<p>27:24 40:14,15,15 40:16 41:1 44:12 45:1 57:5 66:17 70:8 77:7 78:14 79:23 81:10 83:11 84:23 93:20 99:13 99:15,25 100:13 100:20 104:1 113:13 123:19 127:3,16 129:1,2 137:3 145:12 153:2 161:5 165:4 165:5 167:1 168:7 173:8 187:7 189:16 224:12 229:10,25 247:14 248:18 258:15 260:21 participants 70:9 278:4 participate 32:24 participating 3:25 5:5 232:21 particular 12:21 18:3 20:9 21:4 29:18 32:20 36:18 38:19 52:24 68:18 69:21 79:21 90:23 99:23 100:21 150:10 208:7 212:16 213:4 214:9 217:21 218:17 239:21 246:14,21,23,23 251:18 256:7 257:22 262:16,16 266:21 277:2,4 particularly 7:1 33:24 80:21 82:14 86:11 117:24 126:8 129:16 133:5 214:22 parties 79:6 99:4 112:7 144:2,2 151:13 280:8,11 partner 16:14 31:17 40:1,5 142:22 partners 31:14 86:7</p>	<p>103:19 272:10 partnership 44:7 parts 27:8,9 220:3,4 party 11:15 78:7 180:25 pass 15:18 24:6 25:2 passed 186:8 passing 23:17 passive 211:13 passively 251:23 password 255:10 passwords 232:13 242:5 250:8 251:25 patient 219:2 patients 21:19 65:3 219:5 pattern 158:7 patterning 24:11 patterns 18:19 21:12 Paul 68:13 87:2 91:10,13,18 92:4 96:21 99:21 100:20 102:25 103:4 107:19 115:22 118:19 121:13 122:12 125:19 129:13 130:1 132:21 133:13 136:17,18 139:14 273:2 Paul's 139:12 pause 73:24 pay 59:23 61:21 78:14 97:15 115:15 126:14 162:5 168:9 184:13 192:9,11 222:2,5 225:23 226:1 227:10,17 228:7,8 232:18 249:20 259:25 271:6 pay-as-you-drive 169:1,16 payday 249:21 paying 78:18 144:23</p>	<p>213:7 219:17 249:8,23 259:10 payment 11:14 219:20 264:6,11 pays 210:22 Pen 96:3 penalize 128:3 penalty 56:19 penetrate 159:5 people 19:1,11 21:8 21:14,15,16 23:17 23:18 25:6,9,10,20 26:21,22 27:6,6,15 27:16 29:6 31:13 31:18 32:8,10 39:22 41:13,18 42:6 43:4 44:1,13 44:19 45:16 47:3 47:13 48:22,23,25 49:5,7,12 52:5,13 53:1,22 54:3,23 55:1,6,9,21 56:13 61:3,5,10 64:17,20 64:25 66:6,22 69:4 70:4 74:20 75:4 76:16 77:15,17,18 82:4 83:15,15,21 85:6,7 89:9,22 90:22 96:15 97:12 101:17 102:13,18 102:22 106:2,5,8 107:13 117:13,14 125:8 128:19,21 134:20 136:14 139:10 150:18 153:1,3 162:1 165:15 167:4,13 167:19 168:9,16 169:10,15 170:1,2 172:6,18,25 173:11,12 174:3 174:12 175:17 176:8,20 177:14 177:16,22 178:1 178:15,15,16 181:15 190:21 191:5,8 192:10,11 194:10,12,13,15</p>	<p>196:12 197:15,18 197:24 198:3,3,10 198:16 203:5 205:16,18 211:7 215:9 218:24 219:7 220:7 221:19,22,25 223:17 224:24 225:15 226:15,24 227:2,5,12,14 228:2,3,5,8,14 229:4 230:6,10,18 230:20 232:5,9,13 233:21 234:11 235:15 236:2,8,12 236:23,24 237:7 237:10,22 238:17 238:20,22,24 239:2,5 241:10,22 242:4,5 245:1,15 246:9,10 247:3 251:2,13 252:20 258:5,6,13 259:3,4 259:7,8,10,24 260:3,5,7,8 261:4 263:8 264:5 265:18 272:3 273:17,20 275:10 people's 25:15 27:1 27:4,12 31:2 53:5 59:9 61:2 93:8 198:6 233:15 240:9,22 241:13 perceive 141:9 195:6 238:11 perceived 63:8 percent 40:23 41:4 65:8 124:12,13,20 124:20 126:17,17 144:19 169:5,11 169:17 216:22 217:9 225:12 232:8,14,15,20 236:16,24 237:9 237:22 251:2 253:14,24 254:3 percentage 226:2 254:3</p>
---	---	---	---	---

<p>perception 101:5 132:4 198:7 perfect 159:5 perfectly 65:7 93:10 performance 188:8 202:4 period 27:19 41:16 120:7 216:23 258:11 278:8 periods 60:4 156:24 permeating 257:4 permissible 46:7 101:10 128:6 permission 49:13 80:8,12 81:13 155:24 199:10 permitted 4:10 perpetuated 67:8 persecuted 199:14 person 18:8,11 34:1 36:18 44:18 56:21 74:22 79:25 82:23 93:10 100:25 104:12 132:2,8 145:23 158:9 164:7 206:5 231:9 246:12 247:1,11 person's 30:4 49:24 99:18 157:2 personal 12:3,9 15:5 25:8 44:14,15,22 46:12 48:11,11 49:1,12 66:19 109:7 161:6 164:22 189:6 196:12 200:17 210:14 216:1 221:16 222:3 224:16,20 229:16 232:1 236:20 238:19 243:5 249:15 254:1 258:18 259:1 268:4 271:20,24 272:2 personalization 62:25 personalized 63:15</p>	<p>168:15,22 172:18 172:19 173:1,2 178:10 190:11 personally 155:2,18 207:1 208:21 personnel 253:25 persons 215:6 perspective 109:5 160:16,17,18 170:16 212:5,8,13 213:1,19 214:3 215:16 250:22,22 266:2 270:18 perspectives 2:15 8:1 141:3 persuaded 55:16 perverse 262:24 263:5 Peter 14:2 Peters 6:5 pharmacy 70:12,15 70:17 73:6 80:4 90:23 93:3 99:11 philosophers 87:9 philosophical 89:2 phone 17:20 18:5 25:22 28:9 31:7 41:2 53:6 64:13,14 80:9 117:9 170:6 192:20,23 255:11 phones 3:18 31:3,23 80:6 96:2 photo 23:6,11,12,12 24:16,16,16,18 photograph 238:21 photographed 5:3 photos 12:9 physical 32:5 38:17 41:13 43:1,15 79:25 physically 39:25,25 physicians 46:12 PIA 148:20 pick 45:18 160:21 238:10 263:7 271:3 274:18 picked 95:2 picture 20:20 48:1</p>	<p>133:9 140:5,13 189:3,11,18 214:21 251:5 piece 55:13 80:10 84:25 119:14 147:11,14 182:12 185:14 186:11 214:21 218:15 piecemeal 59:7 pieces 55:14 pile 27:6 158:17,18 pill 19:11 pillars 165:3 pin 193:6 ping 80:9 pinged 80:6 pinpoint 36:17 120:2 167:23 265:24 Pinterest 193:5 pitch 266:15 pivot 21:24 pizza 28:11 230:3,4 230:5,6,9 place 4:5 24:17 36:5 47:13 69:1 83:5 100:22 103:21 113:23 128:20 151:19,20 160:24 182:13 222:11 224:24 226:24 229:9 264:7 265:1 265:2 273:6 275:24 places 16:18 44:21 47:12 53:21 54:1 159:4 169:2 202:14 placing 160:3 225:21 plaintiff 93:23 plaintiff's 96:7 plaintiffs 94:2 plan 3:24 53:14 plane 43:15 planner 190:10 191:2 207:4 planning 15:11,14</p>	<p>plastic 4:12 platform 27:24 63:15 172:9 179:14 platforms 58:11 63:1 plausibly 92:8 play 31:3 63:24 81:5 130:4 132:6 203:18 242:12 players 158:23 playing 29:10 128:24 132:6 138:20,22 Plaza 4:3 pleading 122:15 please 3:17,19,21,24 4:9,14 5:1,2,17,19 5:23 146:21 174:1 185:2 202:6 207:10 210:9 278:15 pleasure 39:12 plenty 50:11 52:11 52:21 plug 164:1 plus 23:8 250:1 pocket 19:12 259:10 pockets 20:2 point 10:6 23:10 38:7 40:1 59:3 60:25 62:21 69:21 70:10 73:11 74:21 75:1,7,13,21 77:6 77:14 84:12 87:18 91:6 92:9 94:22 97:3 99:8 107:20 111:11,17,20 114:13 118:1 120:24 121:8 123:2 124:14 126:10,15 127:12 129:15 130:18,23 133:11 134:8 138:7 156:6 159:21 168:5,18 179:2 185:11,25 185:25 207:3</p>	<p>214:4 215:11 217:1 245:22 251:15 253:2 255:9 256:14 259:1 275:10 pointed 86:10 87:16 108:2 114:3 132:15 188:20 191:4 pointing 108:6 points 125:21 130:10 155:12 276:3,22 police 18:7 28:17,23 51:11,11,15,19,20 214:17,19 215:3 policies 122:8 138:22 163:5,6 166:13,22 168:2 171:4 173:21 179:17 180:2 186:19 187:13 198:2,14 202:1 221:12,16,20 224:14 225:22 259:5,15 270:15 policing 50:22,23 policy 7:21 8:22 9:19 10:6 16:7 69:3,3 70:3 142:14 142:16,19 143:5 167:12 168:5 183:23 209:20,23 220:3 231:14 242:15 247:6 248:10 264:7 274:11,15 Policymakers 10:10 polite 134:10 political 138:12 222:20 politician 40:11 polluted 213:23 Ponemon 220:17 pontificate 83:10 pool 90:5 poor 78:22 pop 184:10</p>
---	--	--	--	--

<p>popovers 176:3 popping 20:14 178:8 popular 19:8 population 20:16,18 21:22 28:2 90:13 90:17,17,18 100:21 229:9 251:4 259:4 260:11 populations 100:18 populos 20:12 popunders 176:3 porn 12:7 59:5 272:9 portion 214:18 244:9,11 portions 45:11 portrayed 87:19 pose 170:19 188:4 225:15 poses 18:15 209:17 position 45:17 55:18 131:6 234:3 positive 45:7 46:23 52:8 86:9 95:20 160:25 240:9 244:6 Posner 108:2 possibilities 54:18 possibility 72:25 119:4 201:19 237:13,15,20 238:4,8 possible 6:4,21 32:21 54:17 65:6 110:18 126:18 128:20 139:5 148:21 160:5 161:9 198:3 224:13 225:17 226:12 228:17 249:7 258:3 275:23 possibly 85:22 192:18 224:1 post 212:5,7,13,21 215:16,24 243:4</p>	<p>244:16 250:22,23 251:7 postal 40:9 posted 5:6 25:18 26:3 29:23 31:12 posterior 124:11 posting 12:8 59:9 posture 103:7 104:23 potential 2:11 12:16 13:19 33:9 34:12 68:1 73:12 76:6,12 97:18 128:9 141:11 146:8 147:12 154:11 160:8,13 233:6 245:5 265:7 266:17 273:18,21 274:3 275:14 potentially 37:20 66:6 67:9 104:8 111:15 122:11 231:21 235:5 257:17 275:18 power 150:20 200:18 202:19 206:9 247:22 powerful 9:20 265:6 practical 64:16 137:6 234:6 practice 12:19 16:17 133:23 156:25 161:5 180:24 212:17 213:16 235:24 251:11,18 255:14 274:4 practices 8:21 9:22 10:12 58:20 112:8 128:4 138:22 141:14 145:20 148:10 150:11 151:4 156:12 157:6 168:6 185:8 185:10 186:13,14 188:17 194:24 195:1 199:24 205:13,16,20 241:2 270:16</p>	<p>276:12,24 277:2,3 277:17 pragmatic 64:6,10 64:16 precautions 160:23 precedents 128:5 precisely 10:13 242:17 predict 8:22 102:18 predictably 217:17 218:1 predicting 158:9 prediction 77:9 predictive 50:22 predictor 241:1 preexisting 92:25 93:1 prefer 63:8,19 97:14 144:21 168:11 preference 229:7 237:16 239:22 241:19 preferences 9:2 72:18 140:16 179:8,13 190:23 199:2 222:9 225:5 230:8,15,16,21 231:3,22 233:18 233:19,24 234:6 235:17 236:3,6 239:13 240:22 241:11 242:20 257:16,16 prefers 43:23 pregnancy 34:4 premise 121:5 premium 184:12 194:8 premiums 169:8,23 presence 148:16 present 22:5 68:23 189:10 223:17,24 presentation 24:13 presented 63:14 179:23 189:18 208:19 presenting 228:2 presents 190:15</p>	<p>president 16:11 142:9,13 pressures 247:8 pretend 223:17,25 225:11 pretexting 53:6 pretty 40:22 51:24 62:10 82:5 89:12 102:12 129:14 131:22 143:18 160:19 165:19 181:7 196:5 215:11 232:4,6 244:6 248:14 252:22 254:25 262:1 269:1 276:16 prevalence 41:8 216:17 266:20 prevalent 185:15 prevent 10:1 37:5 67:7 79:5 105:20 105:23 106:2 216:12 227:11 232:1,19 255:6 277:24 preventing 57:22 255:20 preventive 262:7 prevents 254:24 preview 35:22 previewed 229:1 previous 118:20 122:12 194:5 208:7 221:24 251:25 267:9 268:6 270:20 previously 33:3 prey 112:8 price 206:11 210:22 221:12 226:2 250:4 264:20 prices 221:3 223:22 249:17 pricing 35:11,15 pried 211:6 primarily 142:6 222:18</p>	<p>primary 8:9,18 240:6 Prime 90:21 Prince 226:23 228:7 228:9 237:4 256:18 principle 79:21 112:24 136:25 138:20 principled 10:14 principles 81:22 135:11 138:16 152:8 print 170:5 prior 123:18 priorities 142:11 195:6 prioritizing 187:3 priority 162:14,20 162:25 164:5,11 164:12,15,15 priors 124:1,6 prison 106:22,24 pristine 211:15 privacy 3:11,13 6:2 7:5,6,8,13 8:7,10 8:15,17,18,25 9:13 10:7,16,21 11:6 12:18 13:1,7,10,14 14:4 15:23,24 16:4 16:8 17:2 27:12 41:19,20 43:18 61:11,14 68:3,23 69:22 70:11 72:9 72:13,14 73:17 75:9,11,20 77:6 78:2 79:3,8,20 80:2,20 81:6,6 88:17,18 89:14,16 89:25 90:4,13 103:24 104:2 107:25 108:2,22 109:25 112:2,24 120:15 132:3 133:7 135:7,24 138:7 139:20,21 140:2 141:13 142:16 143:7,9</p>
--	--	---	---	---

<p>148:17 150:14 152:8 153:24 154:16 158:25 159:7,8,11,20,22 161:21 162:23 163:24 164:5,12 164:15 166:13,22 167:2,7 168:2,8 169:3,9,14 170:11 175:2,17 177:20 177:20 179:19 180:2 183:12 187:11,13,16,21 187:25 188:8 189:2,4,9,15 190:6 191:8,9 192:15 193:14 194:1,6,23 195:1,10,11,21 197:2,19 198:1,2,4 198:11,14 199:12 199:15,20 200:2 200:22 201:1 202:1,4 206:21 207:6 208:20 210:11,14,18,23 211:3,18 212:2 218:3,8 219:4 222:17,23 224:4,5 224:9,13 225:8,21 226:3,3,10 227:15 228:5 229:4,5 230:8,11 231:2 234:20 235:4,8,19 235:23 236:7 237:17,25 238:1 239:5,14 240:22 240:25 241:2,11 248:10 256:18 257:3 267:10,17 271:19 274:13 275:15 278:14 privacy- 8:12 privacy-enhancing 195:16 privacy-protective 131:8 privacy-related 176:9 243:2</p>	<p>PrivacyCon 278:15 278:17,22 privacygrades.org 188:9,12 private 25:16 43:24 44:16 61:6 74:10 74:16 77:25 78:4 103:23 136:1,14 139:3 140:3 168:16,17 179:20 211:6 271:20 privilege 273:8 prize 189:8 proactive 166:16 proactively 176:17 probability 70:21 277:10,13 probably 17:19 25:16 26:9 27:2 28:7 31:15 32:9 73:24 79:15 84:6 88:21 99:10 111:8 111:19 112:20 115:20 118:6 123:13 147:9 154:1 164:24 168:11 181:10 213:14,18 231:10 234:22 237:18 239:7,9 246:18 249:10 251:7 255:1,8 259:2 261:11,17 267:13 problem 18:8,25 47:18 60:20 65:2,4 65:9,12 97:22 98:1 107:23 116:22 123:14 125:15,18 131:13 136:17 209:3 254:6 267:10,11 277:22 problematic 42:11 55:2 98:3 114:17 115:12,18 133:19 247:19 problems 50:17 60:21 97:7 125:24 135:8 137:5 187:4</p>	<p>243:15,17,18 273:1 proceed 4:23 94:4 194:14 Proceeding 3:3 proceedings 280:5,8 process 9:7 33:7 45:12 58:7 72:14 164:2,3,9 165:6 processes 58:17 163:19 procure 19:2 product 24:19 39:15 71:9 100:13 181:2 187:25 210:23 224:6 248:21 249:8 267:12 products 58:19 155:4 173:23 187:16,18 189:11 189:12,22 190:6 190:13 191:23 195:10,11,14,16 195:17,21 199:4 206:19,20 223:11 223:11 257:19 258:5 272:5 profession 72:10 245:13 professional 171:9 professionals 18:22 154:16 professor 16:1 101:3 142:1 188:6 196:25 208:23 209:13,13,20 222:19 profiles 26:1 27:5 profit 275:3 profitability 184:7 profound 21:12,18 50:6 profoundly 59:25 program 3:16 6:3 16:16 41:17 44:13 165:3 programs 41:5 progress 34:23</p>	<p>210:25 prohibit 105:25 106:1 prohibited 169:2 project 16:13 34:14 35:21 39:1 40:17 219:15 220:6 proliferated 161:14 promise 119:6 224:9 225:25 226:6 248:8 promised 60:7 210:19 promises 210:20 promising 251:16 251:19 252:22 promote 34:5 35:19 209:18 promoted 174:20 prompted 212:2 prong 11:4 proof 131:2 proper 12:18 property 208:18 215:18 proportion 232:5 proportions 22:1 protect 8:20 9:13 54:24,25 89:8 131:5 135:18 158:20 170:12 183:12 190:16 191:21 205:23 218:3 225:23 230:20 235:24 248:18 260:9 protected 57:20 58:1,4 66:19 162:18 175:2 179:24 240:25 247:23 protecting 13:21 35:4 82:1,1 134:3 137:12 138:9 159:22 224:24 260:1 protection 1:2 3:11 3:14 6:24 17:2</p>	<p>20:8 35:3 42:16 68:4 72:13 108:3,9 109:4 142:7 151:10 153:9 163:10 194:1 208:17 209:25 210:19,23 222:5 226:3,4 259:12 264:5 270:10,11 270:13 271:15 protectionist 112:25 protections 191:6 201:4 207:6 256:1 264:7 protective 103:24 179:19 protects 9:9 protest 228:6,13 237:22 protestors 199:17 protocols 117:11 proudly 39:13 provable 108:18 prove 22:19 24:22 45:24 120:22 provide 10:18 14:10 15:8 33:18 44:7 56:17,19 63:17 184:6 187:18 200:4 206:17,20 233:3 provided 4:18 39:11 50:19 53:12,13 192:3 provider 56:16,20 182:4,17 183:3,6 providers 11:13 22:10 182:21 224:18 provides 90:7 providing 6:9 53:24 81:18,19 263:2 provision 135:16 provoked 218:10 proxies 57:13,20 106:12 proxy 57:17 221:6 psychological 242:2</p>
---	---	---	--	---

246:22
public 6:12 15:23
 16:18 25:15 44:21
 45:21 47:12 48:14
 142:14,19 209:20
 261:23
publicly 5:8 33:22
 150:4,8
publish 145:1
published 19:19
 64:13 108:24
 208:19
publisher 176:5
publishing 51:19
 145:10
pull 75:4
pulled 27:11
pulling 150:5
pulse 88:20
punishments 56:20
purchase 94:23
 103:13 224:1,2
 258:8 259:7,19
purchased 70:22
 71:9 85:14 232:16
 259:4
purchasers 258:7
purchases 225:14
 257:19 258:4
purchasing 35:15
 57:16 77:10
 194:10 221:19
pure 20:11 21:6
purely 10:1 62:2
 73:19
purported 233:16
purpose 45:25 89:18
 110:22 153:2
 202:11
purposes 12:14
 42:12 52:8 72:24
 110:25 111:15
 114:8 119:19
 271:24
pursue 235:7,13,25
purveyors 118:8
push 98:25 127:1
 158:13 267:21

276:7
pushed 129:15
 130:2
pushing 129:14
 191:6 278:24
put 43:11 47:2 59:18
 66:1 74:25 87:6
 89:5 95:3 116:3
 121:12 122:23
 125:12 129:5
 131:2,5 134:21
 146:14 151:18
 152:5,16 160:24
 161:10 163:24
 164:5,15,15 171:2
 173:18 175:4
 185:14 192:2
 198:10 203:4
 212:7 240:23
 264:20 270:4
 272:22 275:23
 278:22 279:2
puts 146:9
putting 89:9 162:14
 164:11,18 193:11
 216:19 220:12
 267:3

Q

qualifier 74:9
qualifies 70:5
qualitatively 7:11
quality 50:8
quantifiable 18:16
 20:2 72:6 108:18
 119:3 132:11
 145:22
quantification
 242:14
quantified 50:9 72:3
quantify 14:1 18:19
 73:22 120:2
 130:21 137:14
 174:24 175:4
 177:5 196:1 203:1
 244:23 251:9
quantifying 14:6
 74:1 119:10

220:20 225:24
quantitatively 7:15
quarter 232:9
question 5:14,17,23
 5:24 15:16,16,19
 17:4 29:1 56:5
 60:17,23 61:25
 62:1,6 80:24 86:23
 87:23,23 88:17
 91:3 93:16 99:14
 115:1 116:24
 122:25 125:20
 131:22 133:6,9,15
 134:11 140:1,13
 140:13 146:24
 150:8 153:23
 159:24 160:15
 164:19 177:13
 178:4 188:4,15
 190:6 196:24
 200:8 210:5 212:4
 214:10 220:2
 228:21 229:18,20
 229:25 231:4
 234:19 240:2
 242:24 246:16
 247:10 250:14,14
 257:18,24 258:24
 260:2,13,16
 261:17 262:8,11
 264:22 265:4,17
 274:11,22
questionable 113:11
questionnaire 46:5
questions 5:13,20
 15:15 37:7 60:8,8
 63:12,13 72:21
 111:8 123:6
 132:21 133:1
 140:6 141:17,22
 143:18 149:14
 150:1 178:12
 190:12 195:24
 215:12 216:8
 217:5 229:14
 231:23 232:24
 236:21 243:3,11
 243:16 246:6

257:14 274:12
 276:9,10
quick 16:21 31:20
 65:19 89:5 163:13
 194:22 195:9
 210:6
quicken 88:20
quicker 125:11
quickly 20:3 21:24
 61:4 68:7 94:16
 96:20 115:25
 148:8 155:2 156:4
 165:24 175:8
 178:24 258:19
quite 10:6 41:10,19
 86:9 104:18,19
 115:6 134:10
 156:10 166:1
 175:4 190:14
 212:8 229:15
 230:11,13 251:16
 253:5
quo 199:19

R

R 3:1
race 34:4 57:15,17
radiation 257:4
raise 5:18 15:17
 34:7 35:14 37:7
 68:25 69:6,17 70:4
 70:11,14 71:10
 110:7,13 123:2
 141:20 146:19
raised 69:4 71:24
 72:4 74:6 79:22
 81:12,21 91:4
 111:3 113:9,17
 118:18 121:8
 123:1 137:22
 177:12 266:3
raises 70:23 71:12
 82:20 94:8 101:10
 110:16,22,25
raising 70:9
rally 171:15
ramifications 70:2
ran 26:7 38:21 49:6

256:21
random 261:5
range 9:1 12:25 15:7
 35:16 49:16 266:7
 274:20
rank 174:22
ransomware 264:15
 264:20 265:2
rape 51:17
rapid 172:13 196:5
rarely 147:14
RAT 29:21
rate 78:15 172:13
 188:7 196:5
rates 71:12 78:18
 105:12 107:9
 215:9
ratio 124:3
rational 185:1 197:1
ratios 197:22
RATs 30:13
re-evaluate 185:13
reach 100:2 128:10
 145:6 182:25
reaching 145:7
reactions 272:23,25
read 69:15 90:8
 110:6 135:12
 136:19 148:1,19
 210:4
readily 128:17
reading 192:22
ready 38:25 135:6
reaffirm 137:19
real 9:3 20:2 43:3
 53:3 136:5 137:1,1
 137:2 174:11
 178:5 195:9 202:2
 202:2 234:25
 242:9 247:24
 252:8
reality 62:24 147:9
 147:11 253:9
realizable 119:3
realize 42:13 161:4
 167:2 170:1 174:6
realized 42:14 72:3
 72:6 73:5 174:14

<p>213:3 realizing 175:17 231:20 really 17:16 22:24 24:15 41:10 42:2 46:18 49:2 50:7 53:14 54:25 55:18 55:20 58:22 60:1,2 60:19 61:13,13,16 61:22 63:18 65:13 66:1 67:1 68:17 69:2,8 70:1,3 74:12 76:8,12 83:13 84:17,22,24 86:15,17 87:15 92:22 94:16 95:7 97:10,21,23 98:3 98:13 107:6 108:3 114:5,11,16,16 115:18 121:4,22 123:8 124:7,8,8,15 124:16 125:5,20 126:7,8 133:22,23 136:15 137:7 140:3 144:12,12 144:13,24 146:10 148:11 152:5,10 153:19 154:6 155:11,23,25 160:25 162:5,14 163:3,4 164:12 166:9,17 168:19 171:20 172:25 173:18 176:23 177:7,19 179:17 179:17,25 180:18 181:16,20 183:2 183:24,24 186:24 187:2,6,22 188:19 189:1,6,14 190:21 190:22,24 191:9 191:14 193:13 194:12 195:13 196:20 198:11,13 199:3,5,8 200:25 202:17,25 203:22 204:22 205:2,12 205:22 206:16,18</p>	<p>215:1 218:1 225:3 225:16 226:14,14 226:25 229:15,19 230:10,13,19,20 231:15 237:17 238:3,14 239:21 239:23 240:8,9,21 241:19,24 242:9 242:13 243:23 244:25 245:3,12 245:21 246:8 252:23 253:2,19 254:4,16 256:2 257:1 258:20,23 260:9 267:2 271:1 271:16,18 272:6 272:17,19,20 273:7,23 274:9,11 274:19,21 275:20 276:3,4,7,9 277:5 277:6,10,13,14 278:1 realm 21:25 reason 3:22 10:22 44:11 79:22 80:2 97:21 99:13 107:3 113:18 132:14 134:2 137:23 173:19 175:17 176:8 177:6 180:1 187:14 210:20 247:4,14 259:14 reasonable 118:3 132:7 145:21 184:25 reasonably 128:14 145:18 reasons 9:19 19:15 73:23 78:25 79:1,4 81:22,23 103:3 108:21 117:23 118:19 122:11 176:10 179:9 195:14 219:24 234:6 240:6 rebuild 43:9 rebutted 89:6 recall 87:7 194:5,9</p>	<p>receipt 11:23 receive 19:4 80:25 received 4:12 192:19 receiving 179:21 recess 67:22 140:24 207:16 recidivism 51:4 reclassify 198:21 recognition 22:15 214:18 recognize 38:21 85:16 recognized 151:6 154:1 recognizes 9:7 recognizing 108:8 150:19 recommend 55:3 recommending 173:15 reconcile 239:4 record 5:12 9:16 43:5 53:25 106:17 174:21 201:3 213:7 249:20 recorded 5:3 280:5 records 12:4 21:14 21:17 40:16 41:25 42:1,1 43:3 46:15 53:6,18 113:21 168:22,25 174:15 180:22 219:6 245:17 250:7 252:4,6,7 recourse 19:17 82:23 93:22,23 red 27:15 159:17 redress 118:7 redressable 94:7 117:25 reduce 55:2 83:3 122:9 149:23 213:18 reduced 227:18 241:8 280:6 reduces 10:7 124:18 reducing 89:16</p>	<p>reduction 78:19 169:5,11,18,18 reductionist 72:7 refer 73:13 reference 200:11 216:23 referenced 246:17 referring 94:14 reflected 125:19 refund 226:4 refunds 11:23 refused 55:6 regard 224:5 225:6 regardless 45:7 77:9 161:6 regime 92:15 regions 19:22 Register 96:4 regular 180:22 236:7 regularly 232:6,13 Regulate 108:17 regulated 149:21 154:8 157:17 regulation 102:4 165:23 218:14 regulations 200:23 201:4 209:17 218:9 219:4 regulator 108:14 regulators 121:2 151:6 177:7 188:23 200:4 262:22 regulatory 104:23 160:4 200:22 201:24 278:1 reiterate 91:17 reject 126:22 relate 109:17 related 16:9 82:10 97:21 104:1 124:5 160:20 190:5 208:19 210:10 219:11 232:24 243:3,9,17,18 280:7 relating 210:3</p>	<p>relationship 13:15 45:9 84:20 99:1,4 99:5,6 112:8 155:21 176:21 186:23 210:18 244:6 253:18 relationships 40:4 44:23 48:11 84:1 97:12,16 151:12 relative 38:15 186:9 187:7 195:3,4 280:9 relatively 221:15 relatives 54:13 release 25:15 released 18:17 42:12 190:10,19 242:7 relevant 13:14 86:23 126:8 215:20 216:4 217:13 reliable 223:6 225:4 relocate 53:16 relocated 53:10 relocation 43:15 relying 50:22 261:22 remain 4:1,8,17,24 remains 21:1 192:12 remark 66:10 remarkable 215:11 remarks 2:3,6,19 3:4 6:14,16 14:11 201:12 269:5 270:1,4 remedies 24:7 56:2 56:2,8 57:3,8 242:15,17 275:14 275:23 remedy 47:9 56:14 56:18,22 87:22 100:5,24 101:11 132:12,13 264:25 remember 4:9 137:4 181:25 278:13 remembered 90:10 reminded 192:13</p>
--	---	---	---	---

<p>reminder 141:18 remote 29:20 30:1,2 62:8 remove 21:17 rendered 89:17 renders 109:10 rent 37:25 reopen 4:8 repeat 125:22 repeatedly 80:6 134:12 repercussions 117:6 rephrased 257:25 replace 82:17 report 18:17 20:21 21:16 34:11 50:13 59:18 117:17 192:7 221:1 reported 1:25 214:20 256:10 reporter 42:13,18 42:22 280:1 reporting 209:25 260:17 262:12 263:13,14 reports 12:11 20:10 21:5 139:21 176:18 187:14 206:16 220:10 232:15 233:25 represent 44:13 143:25 144:1 150:17 178:16 representative 177:23 240:3 representatives 109:23 representing 16:19 represents 27:16 reproduce 50:24,25 reputation 57:1 94:19 reputational 150:13 196:1,4,8,9 require 24:9 37:8 166:24 263:14,14 required 45:17 162:2 165:5</p>	<p>requirement 262:17 requirements 145:25 152:3 262:12 requires 4:16,19 92:24 127:2 research 15:23,25 16:3 17:15 19:19 21:15 23:10 25:13 34:6 39:24 42:12 50:21 72:9 165:19 171:19 209:1,14 209:22 210:10 211:1,17,25 215:10 217:19,21 218:1,6,11,15,16 218:19 219:1 222:21 223:6,15 223:16 231:15 236:8,15 244:15 245:3,7,24 251:16 252:23 254:14,23 263:18 265:12,14 267:14 270:15 271:9 272:18 276:4,6,9 278:14 278:21,22 researcher 110:10 266:10 researchers 238:2,6 249:12 251:20 263:22 residents 19:23 209:10 232:20 resist 198:5 resolution 156:11 resolve 244:10 resource 163:25 256:10 resources 10:1 50:23 respect 86:10 136:13 152:1 182:6 respected 15:24 179:14 respectful 3:19 respond 49:19 91:2</p>	<p>91:13 113:13 116:19 121:10 127:22 133:15 156:4 165:23 178:25 261:23 respondents 223:9 236:17 253:12 responding 87:5 response 28:17 132:24 195:5,7 210:6 215:9,14 216:8 230:14 responses 129:12 230:23 244:16 253:11 responsibilities 68:20 responsibility 109:10 150:20 151:16 157:6 responsible 35:19 133:23 135:17 146:15 151:3 153:6 202:18 209:7 213:25 260:1 responsibly 118:9 203:5 rest 81:21 160:20 203:4 204:12 262:5 restaurants 47:14 resting 71:7 restrict 186:9 restricting 13:21 restrictions 10:9 146:9 151:23 restrooms 4:2 result 15:4 43:21 115:13 218:20,23 244:17 245:6,14 247:11 resulted 11:19,22 28:20 243:15 results 45:7 101:6 134:25 185:20 189:25 191:4 212:9 225:16</p>	<p>retail 70:12 71:22 90:9,16 94:25 96:22 105:6 retailer 213:15 retailers 95:25 219:20 retain 90:5 retroactive 200:16 return 4:14,25 11:21 168:4 reuse 4:13 reveal 33:21 75:7 159:14 270:23 revealed 74:13 75:14 85:6 230:16 233:18 239:22 241:19 257:16,17 revealing 61:2 77:6 77:14 revelation 77:17 86:5 revenge 12:7 59:5 272:9 revenue 173:3 176:5 revenues 144:8 reversed 191:7 review 3:17 108:24 191:8 reviewed 35:23 reward 229:10 RFID 95:2 rich 89:21 richer 127:13 richness 187:20 rid 157:4 199:25 ridiculous 132:17 right 4:2 22:20 29:1 36:15 41:2 55:17 59:2,8 76:1 81:7 82:16 83:22 85:6 86:2 87:11 88:2,6 88:18,22 90:2,14 91:21 93:24 94:2 94:16,21 95:3,20 96:4,11 99:6 100:5 102:6 103:7 114:24 116:9,18 116:21,24 117:14</p>	<p>118:4,23 119:7 127:14 128:15,22 131:18 132:23 134:15 135:3 136:9,18 137:17 141:4 143:7 146:24 150:12 153:9 162:16 163:1 164:7 173:19 176:14 189:3 192:16 194:18 199:25 204:18 205:16 215:8 217:15 219:8 222:6,9 229:12 230:13 234:25 242:3 251:3,11 255:14 256:9 259:16 262:5 264:5 266:16 267:2 273:2 274:23 275:2,3,8 277:7 278:23 rightly 156:17 rights 34:16,17 36:24 56:12,12 96:15 132:9 rigorous 134:17 164:8 rise 60:13 risk 7:16 13:15 21:21 23:18 36:7 42:7 81:5,11,14,15 82:20 83:3 84:22 84:23 85:13,18,20 88:1,9,11,25 89:9 89:16,25 90:4 91:19,20,25 92:6,7 92:19,25,25 93:12 93:14 95:14 97:25 99:17 100:11,12 101:11 105:8 111:12,19 114:13 115:7,8,11,16 119:5 122:9,24 124:21,22 125:21 126:1,13,16</p>
--	--	---	--	--

<p>127:19 128:12 129:1,2 130:16 132:10 144:14 147:3 148:23 149:7,19,23 150:7 153:17 156:20 161:22,24 187:3 202:24 212:15 213:2,3,18,23 214:2 216:17 231:8,9 239:9,11 245:22 250:16 251:9,10,12,14 256:7,8 257:10,12 259:11 266:25 273:14 274:3,3 277:3,8,13 riskier 88:6 risks 7:18 8:2 9:8 13:4 18:16 34:12 50:25 52:3 141:10 143:20 144:4,5 145:12 146:10,12 147:5,17 148:14 148:20 149:2,5 153:19,23 154:2,6 154:12,13 160:2 161:8 164:21 167:25 170:17 183:18 200:12 202:21,24 231:6,7 259:17 275:14 277:6,23 RMR-CRR-CLR 280:18 RMR-CRR-CLR-... 1:25 road 159:17 277:9 rob 239:8 robust 190:6 Rochester 209:21 rocket 193:5,13 rogue 18:24 role 8:6 102:5 130:4 132:6 138:18 242:12 roll 50:10 rolls 263:11</p>	<p>room 4:17 26:22 47:24 48:3 88:19 117:7 183:11 184:17 219:7 rooms 18:6 roster 20:13 rough 226:14 routinely 59:15 row 201:10 237:4 rubric 95:7 96:12 99:16 101:3 ruin 41:23 117:13 rule 137:11 162:4 191:8 rulemaking 200:18 rules 9:11 102:6,23 194:6 203:20 260:17,22 rummage 30:5 run 19:10 35:10 38:20 43:8 63:24 71:23 249:21 running 41:13 53:22 runs 62:23 256:20</p> <hr/> <p style="text-align: center;">S</p> <hr/> <p>S 2:1 3:1 S.W 1:14 s/Susanne 280:17 sacrifice 178:7 sad 196:10 sadly 94:17 safe 41:17 42:6 54:14 182:9 safeguard 63:23 safeguards 151:18 151:20 safely 54:18 safer 169:10 safety 13:4 16:13 39:15 40:17 53:14 267:12,12 sales 142:4 sample 215:5,8 240:3 sanctions 56:19 Santa 222:20 sat 34:9,20</p>	<p>satisfy 204:4 saw 169:11 173:15 191:6 199:1 237:1 241:5 saying 8:9 14:2 46:11 49:9 57:10 75:2,24 78:22 91:22 100:1 101:14 117:8 127:3,24 135:7 138:6 147:6 177:21 194:14 203:9 220:11 235:11 238:1 254:11 260:20 says 77:1 84:15 94:23 106:16 126:1 159:17 181:21 192:23 234:13 237:17 241:18 scalable 245:13 246:1 scale 32:14 scan 22:14 23:5 scanners 94:25 scary 180:17 181:15 scenario 53:9 72:5 72:20 73:3,4 80:18 109:13 118:21 120:16 204:9 scenarios 12:1 21:18 scenes 181:7 schedule 4:1 scholarly 72:8 scholars 87:10 108:1 scholarship 134:23 139:18,22 school 16:2 108:1 116:4 142:3 209:14 243:16 259:22 schooling 259:20 schools 22:10 science 16:2 222:20 251:21 252:21 science-based</p>	<p>253:21 sciences 72:11 134:22 scientist 252:19 scientists 161:18 245:9 scope 66:8 score 126:6 188:10 scores 51:4 screen 36:11 38:18 69:16 screening 236:21 screens 61:4 se 80:1 139:5 search 42:12,19 searches 31:20 searching 42:15,15 61:3,5 seats 141:5 seclusion 13:5 76:19 second 7:13 10:22 12:16 13:9,17 27:24 61:25 62:1 93:14,15 96:12 109:6 120:6 126:23,23 180:7 212:6 217:25 268:9 272:20 secondly 130:14 176:23 seconds 130:24 139:11 secret 78:13 Section 8:19 9:11 10:24 70:2,5 136:19 145:17 sector 60:2 149:14 149:15,16 154:8,8 203:16 sectors 33:8 148:7 203:15 secure 24:15,16,18 114:22 158:16 159:4 182:17,20 182:21 183:3,13 secured 275:19 securely 24:18 182:14</p>	<p>security 3:23 4:4,13 5:1 6:2 7:5,9,13 8:7,10,15,18 10:16 10:21 11:7 12:18 13:1,7,11,15 14:4 16:4 35:7 41:20 43:18 53:4 55:8,10 65:4 68:23 98:1 110:3,9,10 111:6 114:17 117:5 118:4,6,8,16 126:3 128:6 141:14 143:8 149:11,22 160:16,18,20,23 160:25 162:10,12 163:9 170:21,22 174:19,22 181:13 181:18 182:9,12 182:13 185:8,10 187:11,17,21,25 189:2,4,9,11,15 190:10,25 191:2 193:14 194:2 195:3 196:10,13 197:2 199:20 201:1 203:10 204:1,23 206:21 207:3,6 209:21,23 209:24,24 210:1 210:12 212:2 218:24 219:4,13 219:16 238:23 245:5 249:16 258:19 259:18 261:25 265:7 266:5 267:11,18 271:18 274:13 278:14 security-related 8:12 see 3:8 6:3 20:4,12 20:14,21,22,23,25 21:9 22:21 23:8 26:17,23 27:14,19 28:1 31:11,24 36:10,14 39:9 42:8 43:18 44:19 46:18 47:12 48:18 52:5</p>
--	--	--	--	--

52:12,15,25 54:22 55:20 56:8 61:3,14 67:20 74:20 75:5 83:4 92:17 93:11 96:8 97:7,21 100:8 102:15 111:1 113:9 114:9 124:1 125:8 137:24 138:13 163:6 181:5 184:24 185:20,20,21,21 192:3,5 195:13 198:11 199:21 205:6 207:1 216:15 219:7 220:1 222:2 223:13 224:24 227:14,20 229:6 231:8,15 233:24 235:22 236:8 240:9 247:15 251:16 257:7 261:13 265:23 266:24 267:13,15 271:19 272:2 274:9	segue 133:11 seized 263:3 selection 7:21 78:19 self 38:15,15 72:15 72:16 117:14 self-chill 117:14 self-insure 122:8 self-regulation 145:13 161:11 165:21 self-regulatory 146:7 148:5 151:21 153:7 self-reported 220:13 220:18 242:12 self-reporting 233:25 sell 23:1 89:23 238:18 246:9 249:5,14 selling 12:3 70:17 139:9 174:17 221:16 seminal 107:25 Senate 39:17 send 28:18 53:12 102:19 180:22 183:10 237:25 sending 220:10 senior 35:12 208:15 sense 38:14 79:24 84:15 88:2 100:7,9 122:17 126:19 130:2,21 132:12 138:18 147:10 167:25 178:13 194:1,3 213:19 214:2 235:18 260:8 261:3 276:14 277:20 sensitive 11:13 12:8 30:9 34:3 77:11,15 82:14 95:5,10,16 99:20,21 102:13 103:5,5 105:5 151:22,24 155:12 155:13 194:25 214:23 229:16	230:11 sensitivity 43:5 82:12 152:3 154:24 sensors 204:11 sent 48:14 180:21 237:2,7 sentence 71:21 110:6 sentences 48:20 71:16 separate 24:4,5 34:24 50:15 136:12 156:21 171:4 separating 67:2 September 7:6 Sequoia 11:12 series 11:11 231:23 243:3,10 serious 21:12 39:20 94:10 97:22 116:8 154:5 203:2,22 seriously 8:11 serve 12:14 152:12 181:21 served 142:13,15 143:9 server 77:19 183:8 serves 91:23 209:10 service 33:15 40:24 62:25 63:17 100:14 168:22 172:5,22 173:1,2 179:19 181:1 184:8 187:5,6,24 223:18 224:13 232:17 236:18,22 236:25 237:11 248:25 249:9 services 16:16 17:21 19:3 34:5 38:13 44:7,13 61:13 144:11,23 145:10 168:15 172:18,19 172:23,24 176:7 179:9,12,21 187:16,17 188:5	190:7 206:19,20 206:22 223:16,19 223:24 224:2,14 236:16 237:14,24 serving 146:1 153:22 208:24 SESSION 141:1 set 36:1 42:14,20 57:7 58:16,21 63:14 68:15 82:6 85:24 146:6 220:22 223:10 259:23 sets 33:21 39:4 40:15 129:12 159:13 setting 10:20 171:15 187:5 198:11 226:17 229:18 230:1 260:18 settings 27:12 settle 219:21 settled 63:13 seven 73:10 77:5 84:15 seventies 108:1 215:10 severely 217:10 244:9,12 257:3 severity 276:17 sextortion 30:8,14 sexual 39:21 43:22 44:2,17 62:17 86:7 94:20 sexually 40:7 shampoo 57:15,17 shape 205:9 shaped 35:1 share 17:15 119:24 143:22 144:18 160:12 170:17 183:1 195:2 204:3 224:15,21 225:1 237:18 238:1,9 248:10 249:1 shared 33:23 34:2 43:10 180:11 201:16	shares 237:11 sharing 7:18 8:2 13:23 55:7 109:4 141:10,15 147:6 167:22 178:19 180:17,19,21,24 181:15 183:7,19 192:8 199:9,13 237:19 sharpened 147:17 shelf 95:1 shelter 41:17 42:16 64:12 shelters 41:14 shield 8:17 89:8 shields 170:11 shift 35:16 182:19 255:3 260:2 264:14 shoe 152:12 shoes 157:3 193:10 shop 250:2 shopped 63:16 shopper 181:19 short 29:21 108:7 111:7 116:1 158:2 shortcut 65:21,22 shorter 158:6 shorthand 95:9 shortly 269:4 shoulder 76:13 show 21:7 28:4 32:3 47:25 102:2 107:6 131:10 162:16 256:20 278:16 showed 48:20 59:2,4 showing 20:16 54:2 61:2 172:25 190:20 shown 140:8 shows 19:19 48:18 171:19 178:4 196:17 223:22 224:19 256:15 shut 54:3 61:17 184:1,8 side 9:24 89:14 91:10 98:12
---	--	--	--	--

100:10 103:16 139:24 161:1,24 171:7 173:3 177:21 245:1,25 254:22 271:15 sides 147:16 sign 172:6 signal 182:20 228:10,14 238:1 signaling 106:3,5 237:20 significant 8:21 40:13 41:18 50:20 51:1 63:10 93:24 93:25 94:17 95:5 97:24 112:10 113:24 144:25 significantly 162:16 182:24 silence 3:17 Silicon 166:7 silver 65:7 similar 81:22 118:19,20 211:18 similarity 267:10 Similarly 13:22 213:15 simple 18:5 20:10 21:5 121:1,2 159:15 183:24 184:3 simplify 198:1 simply 184:9 241:13 single 65:7 80:14 87:17 97:17 161:20 188:10 site 175:12 181:11 190:20 sites 5:8 28:5 59:5 195:1,2,5 272:14 sits 168:20 sitting 164:7 167:2 188:16 231:19 situation 18:3 28:13 28:13,14,16 55:20 99:10 132:4 158:3 185:11 224:7 situations 18:24	24:8 28:20 154:10 204:14 212:17 233:6 238:9,10 six 8:14 40:4,7 76:20 84:25 244:7 257:8 six-week 27:8 size 157:14 215:8 skeptical 166:21 171:3 195:12 201:16 skepticism 221:24 skeptics 177:20 skew 26:18 skewed 132:15 skills 276:6 sky 211:1 slashed 43:17 slaves 29:25 sleeves 50:10 slice 230:5 slide 20:5,20 21:5,14 22:20 25:17 26:2 27:2 28:7 29:16 30:7,23 35:23 39:11 70:11 110:8 slides 17:9 20:3 slight 63:10 slightly 73:5 150:6 221:5 235:8 Sloan 209:12,14 slow 159:20 small 80:10 81:6,9 120:3 124:10 133:14 148:17 158:17,18,18,19 160:23 164:3 221:15 231:11 254:3 256:12 259:3 260:11 277:10 smaller 60:22 163:23,23 164:14 218:12 244:11 smart 96:2 159:3 255:11 smartphones 192:17 192:17 Smith 3:15 6:21	16:7 32:23 50:18 57:5 62:24 66:24 208:2,3 222:6 228:21 230:24 231:17 233:13 235:18 236:1 239:17 240:11,15 241:16 242:18 244:18 246:4 248:1 250:11 252:24 254:7,19 256:3 257:24 279:4 social 5:8 25:25 27:4 27:10 28:5 32:6 37:17 38:10,13 54:4 55:8,9 71:4 72:11,17 85:2,9 86:12,18 127:14 134:22 168:18 172:8 174:19,22 181:13,18 199:17 238:23 249:16 271:21,25 272:3 socially 27:17 29:7 29:17 228:6 societal 37:3 39:22 58:12,16 131:16 135:8 society 35:1 36:19 38:1,5 40:12 54:2 59:1 78:20 79:5 105:16 131:11 272:1 275:9 socioeconomics 16:5 sold 11:13 193:25 250:4 sole 133:20 solution 65:8,19,23 66:6 252:14 solutions 34:23,25 50:15 57:25 64:24 64:25 66:4 67:4 183:12,13 193:4 247:15,17 253:22 solve 50:17 65:1,8 65:12 116:23 somebody 42:14	46:20 47:16 48:7 49:7 53:9 91:25 93:9 121:18 152:14 212:8 237:17 249:24 270:6 273:14 somebody's 45:2,20 64:8 75:2 76:25 211:16 249:15 264:8 someone's 28:12,18 28:19 29:9 31:7 76:13 249:18 someplace 52:14 279:3 somewhat 113:11 133:2 230:3 Sony 242:7 sooner 278:18 sophisticated 161:18 sorry 67:17 69:24 123:23 129:7 137:22 146:22 150:24 153:14,16 156:4,15 240:14 sort 33:17 34:13 36:24 37:2 38:24 42:21 43:4 51:10 53:9,16,25 54:1,2 54:5 57:23 58:8,12 58:19 62:23 63:3 63:23 64:4 66:25 67:3,8 71:16 78:3 80:21 81:22 83:14 86:1,20 89:7 91:17 92:6 96:21,22 97:15,21 98:8 101:1,2,6 102:16 113:12 127:22 128:16,25 129:23 129:24 130:3 132:9,18 136:14 136:24 137:11 160:5 164:19 170:15 213:8 214:24 218:4 219:14 220:1,2,2,6	220:12,24 221:4,8 221:23 222:7,11 228:24 230:4,14 231:13 233:2,14 233:18 234:7,18 234:25 235:18,20 235:22 236:2 239:25 240:2,12 240:20 242:23 243:1 244:1,14,15 244:20,21,23 245:19,22,23 246:21 247:5 248:15 249:13 250:17,18,19 251:5,8,15 252:5,9 252:11,17,21 253:20 257:4 258:7,12 259:18 261:5,19 262:2 263:20 264:4,23 265:4 267:14,16 270:20 271:3 272:12,23 273:5,8 276:8,21 277:25 sorting 262:7 sorts 19:15 22:15 42:8 83:16 97:9 178:8 270:23 276:3 sound 4:20 109:20 185:1 201:18 226:24 228:8,9 256:18 sounded 130:1 sounds 78:21 180:17 262:1 sources 33:5 220:16 220:19 268:19,20 Southeastern 21:2 Southworth 16:11 39:10 51:10 53:3 62:5 64:4 space 133:21 138:11 138:12,12,13 154:25 186:19 189:24 193:11 220:9 246:10
--	--	---	---	---

<p>256:2 271:23,25 272:17 273:6,6 Spam 120:4 Spammer 120:4 span 16:5 speak 15:6 32:24 60:11 117:2 speakers 3:19 speaking 10:22 56:1 101:1 104:11 215:15 speaks 232:2 Special 6:21 specialist 180:21 specializes 208:17 specific 9:12 10:15 10:20 19:22 24:6 24:24 36:17,20 37:1 41:11 70:21 145:15 148:6 214:6 215:24 specifically 9:4 72:2 75:14 146:11 215:18 232:24 263:21 specter 34:7 spectrum 132:10 speculate 92:10 speculative 111:18 speech 7:5 speeds 223:20 spend 15:13 49:25 87:5 120:4 146:11 178:6 221:10 232:18 243:9 244:4,7 260:4,7 274:5 spends 213:11 spent 117:9 217:6 250:7 260:22 spheres 37:19 spider 29:11 Spider-Man 150:23 150:24 spill 226:22 spilled 226:23 256:24 spills 227:10 256:19</p>	<p>256:20 spoke 128:21 258:21 spoken 124:25 spoof 24:20 spoofed 22:17 spot 21:3 spouses 12:5 spread 159:4 spring 267:24 spy 39:11 62:8,9 spyware 30:24,25 41:7 60:21 SSN 118:23 SSNs 110:9 stab 257:23 260:16 stack 220:19 staff 4:15 5:16 6:20 141:19 278:24 stage 6:3 45:9 68:15 staggering 40:8 stakeholders 65:17 stakeholders' 109:14 stakes 177:17 178:5 178:5 stalk 31:8,18 stalked 40:4,5,5 stalkers 12:5 41:5 stalkerware 31:1,25 stalking 31:14 39:16 39:21 43:7 53:15 99:6 stand 135:14 147:14 204:13 standard 10:24 133:24 148:19 187:15 189:13 260:18 standard's 11:4 standardization 261:9 standardize 261:15 standing 38:15 122:14 127:8,8 standpoint 53:7 Starbucks 40:10 stared 25:17 Starr 106:19</p>	<p>start 7:3 15:2 17:3,8 29:9,11 52:10 56:6 60:22 64:3 66:4 75:8 79:22 91:8,9 91:10 98:16,16,17 98:18,20,21 111:3 123:17 124:16 133:13,14 143:17 147:6 160:14 180:14 192:23 201:13 222:8,11 234:3,10 249:3 260:20 263:24 270:5 278:19 started 3:16 16:22 27:22 34:11 41:6 43:3 68:14 86:2 88:20 141:5 171:7 230:11 250:20 starting 14:16 25:14 63:21 71:25 75:7 79:20 95:4 115:4 210:8 247:15 starts 45:2 startup 162:8 startups 163:23 164:15 218:12 state 18:13 20:12 56:9,11 88:4,6 116:21 117:5 260:17 state's 262:16 state-level 24:11 stated 59:15 133:8 198:22 229:7 230:15,21 231:3 233:18,23 234:5 236:6,9 257:16 261:19 statement 144:10 232:10 statements 10:17 116:9 179:24 180:2 232:7 states 1:1 19:25 21:3 59:6 65:14 106:15 138:8 151:9 186:3 186:4,8 261:14</p>	<p>statistical 20:6 106:9 186:10 statistically 159:15 statistics 144:18 196:11 209:5,6 214:17 stats 41:8 status 34:4 45:15,20 58:1,4 82:15,15 103:3,22 104:18 105:10,12,15 152:15 155:7 199:19 statute 135:12 136:21 statutes 9:12 stay 64:20 steal 249:25 255:7 stealing 174:10 steals 30:9 249:9 steer 73:19 stemming 208:20 stenotype 280:5 step 14:11 33:1 67:4 94:9,13 108:17 160:25 176:24 186:16 190:5 203:25 252:11 stepping 59:6 61:11 steps 53:23 73:9,10 stew 274:12 steward 62:4 sticky 108:3 Stigler 108:2 stigma 42:6,23 62:17 94:18 Stivers 2:20 14:8 269:4 270:2,9 stock 221:3 stolen 31:7 174:18 174:23,25 246:17 250:15 251:25 255:17 268:5 stone 164:11 stop 86:17 169:7 171:25 181:12 219:4 stopped 108:7</p>	<p>store 31:3,4 68:21 72:22 80:5,14 90:9 102:19 stored 22:22 23:5 235:2 stores 31:10 70:12 96:1 110:9 118:22 stories 49:5 236:5 storing 7:19 183:8 story 221:5 238:13 straight 101:21 242:21 straightforward 225:4 234:19 235:11 strange 47:3 225:15 225:16 228:2 strategic 78:14 142:11 strategically 119:21 strategies 36:8 39:4 stratosphere 62:19 streaming 223:16 223:18,20 224:12 236:16,17,22,24 237:11,14,24 248:25 249:9 street 1:14 4:22,23 4:23 23:2,14 strength 7:1 strengths 223:3 225:3 227:22 stretch 246:25 strike 85:15 strikes 97:19 137:15 striking 153:8 stringing 23:16 stripe 159:4 stripped 134:5 strong 12:13 194:3 198:7 244:6 264:14 strongest 234:21 strongly 84:21 structured 259:15 stuck 271:1 student 35:12 75:23 239:6,25</p>
--	--	---	---	---

students 241:5	suffering 57:1 120:20	227:7 268:3	230:8,22 231:21	tackle 13:17 14:7 34:10,20 109:19
studied 50:9 197:15 251:22	sufficient 111:12,20 163:10	supposed 87:13,14 126:4 172:25 174:24	232:21 236:17,21 236:23 237:10,24 237:25 239:22 240:2 241:18 244:15 253:10,17 266:6	tackled 38:7
studies 26:5 32:2,13 106:8 107:6 124:16 166:25	sufficiently 111:23 122:15 149:7 162:18	suppress 105:23	survey-based 222:18,22	tactics 41:23
study 24:3,23 26:24 27:8,8,10 30:16 106:18 194:22 198:15 199:22 220:17 229:8,10 229:14 230:17 240:20 242:24 251:19 252:13 260:21	suggest 77:17 130:24 131:1 175:22	suppressing 105:18 107:2,13	surveys 167:19 178:1 222:13 227:7,23 228:12	tag 264:20
studying 174:6 257:18	suggesting 137:21 138:3 194:11	sure 25:12 51:5 52:11 53:16,18 57:19 65:3 66:23 91:16 93:24 99:5 101:25 116:10,11 122:21 146:25 152:17 164:14 165:2 166:10 171:20 173:10 175:4 176:23 178:19 179:1,7,13 182:22 196:20 197:7 203:4 222:16 227:9 233:20 248:3 253:15 256:5 258:15 261:15 263:4 271:6,13 273:10 277:16	survivor 40:11	tail 102:22 145:10
stuff 31:9 59:2 146:20 169:23 193:4 203:22 204:22	suggests 217:10,22 218:11 252:5	surf 148:9 154:13	survivors 54:7	tailed 207:7
subject 22:21,21,23 23:10,11 114:23 114:24 232:11	suicide 12:11	surfaced 161:19	Susanne 1:25 280:4 280:18	take 8:11 23:4 24:13 32:25 33:1 39:10 40:21 46:22 55:18 60:1,19 65:22 86:24 88:3 94:24 108:17 113:5 114:1 115:16 118:14 119:16 120:18 135:17 141:4,13,17 149:12,18 159:19 160:1 166:20 171:21 176:24 178:7 179:2 187:10 190:18 192:24 198:20 200:14 201:10 204:8 206:6 217:1 229:10 236:8,13 239:7 242:8 244:21 245:14 249:21 254:18 255:1 257:23 258:13 260:15 273:20 274:2 277:21
subjected 88:23	suing 219:16,20	surplus 78:20	swarming 188:12	taken 18:2,4 24:16 24:21 67:22 81:13 126:4 140:25 147:18 200:1,2 207:16 233:5 238:21 254:4
subjective 101:4,5	suit 213:21	surprised 34:14 176:22 245:12	swat 28:18	takes 274:4
subjects 23:13	suits 219:23 234:16 234:18	surprising 25:19 216:19,25 229:18 232:6 246:1	swath 40:12	talk 8:7 13:6 21:8 29:24 43:14 44:5 44:20,25 47:11,15 48:10 53:16 70:1,3 73:25 75:12 76:16 83:15 85:24 86:2 91:4 102:11 115:9 115:10 135:7
submissions 278:19	sum 75:16 247:12 276:8	survey 38:24 40:19 41:3 144:19 179:2 191:3 209:9,9 210:21 214:15 215:3,10,17,19 216:22 220:9 221:1 222:21 223:1,8 224:23 225:16 227:20 228:18,20 229:5	swear 229:22,23	
submit 5:6 141:22 278:12	summarize 203:8 267:14	surface 148:9 154:13	switch 111:2	
subsidize 144:11	summer 8:14 278:20	surfaced 161:19	switching 69:9	
substantial 9:25 11:4 128:14 145:16	sun 249:25	surplus 78:20	sword 147:16	
substantive 20:5 37:14 49:23	super-complicated 122:22	surprise 34:14	Symantec 191:25	
subtle 46:2	supercedes 136:20	surprised 176:22 245:12	sympathize 126:5	
suck 90:4	superheroes 150:25	surprising 25:19 216:19,25 229:18 232:6 246:1	symposium 168:17	
sudden 20:18 47:1 193:18	Superman 150:21 150:22	surveil 12:6	Sys 116:12	
suddenly 45:21 134:5	supervising 16:15	surveillance 100:12	system 4:18 23:3,14 26:5,7,10 30:5,17 65:2,5 80:7 87:21 122:5,16,19 127:14,15 219:9 227:8,9,18	
sued 205:8	supervision 280:6	survey 38:24 40:19 41:3 144:19 179:2 191:3 209:9,9 210:21 214:15 215:3,10,17,19 216:22 220:9 221:1 222:21 223:1,8 224:23 225:16 227:20 228:18,20 229:5	systems 16:6 18:23 24:20 30:19,22 38:10 43:16 114:22 116:4	
suffer 7:4 9:22 178:9 196:24 251:2,3	supervisor 46:23	surveil 12:6	T	
suffered 13:6 216:9 242:3	supplement 215:21 216:3,6 253:6 266:15 267:4,5	surveillance 100:12	T 2:1,1	
	supplements 215:19	survey 38:24 40:19 41:3 144:19 179:2 191:3 209:9,9 210:21 214:15 215:3,10,17,19 216:22 220:9 221:1 222:21 223:1,8 224:23 225:16 227:20 228:18,20 229:5	table 5:15 50:4 65:18 87:6 89:6 185:14 204:9 263:25	
	supply 194:4 245:1 245:25	surveil 12:6	tabulate 227:13	
	support 6:6,9 29:8,8 38:10 144:9,10 145:5,9	surveillance 100:12		
	supporting 41:15	survey 38:24 40:19 41:3 144:19 179:2 191:3 209:9,9 210:21 214:15 215:3,10,17,19 216:22 220:9 221:1 222:21 223:1,8 224:23 225:16 227:20 228:18,20 229:5		
	supports 145:6	surveil 12:6		
	suppose 72:3 225:10	surveillance 100:12		

137:4 139:7 145:3 151:7 157:15 168:21 182:11 205:21,22 206:7 210:2 211:10 223:2 228:19 251:9 257:2 259:1	target 61:1 70:25 76:16 167:12 targeted 21:19 26:21 50:23 54:3 76:11,17 90:22 146:1 165:13 172:21 175:10,19 175:22 176:2 181:12,17 targeting 21:23 76:7 76:8 targets 62:21 task 184:25 taste 101:22 tautological 126:24 tax 11:21,22,23 169:19 taxes 227:8 TaxSlayer 8:16 11:21 teaches 142:3 team 192:10 279:2 teams 28:18 tease 240:9 teasing 129:22 237:7 tech 40:25 41:1 58:11 162:7 163:24 164:14 188:20,22 technical 73:23 119:6 171:7 technique 201:24 techniques 248:20 technological 57:25 67:9 253:21 technologically 95:12 technologies 9:9 12:15 58:24 67:10 97:3,11 195:16 Technologist 68:5 technology 8:25 10:5 11:24 16:14 23:6 37:4 40:17 41:6 54:19 55:16 55:19 57:11 63:2 64:7 66:12 67:5	68:11 69:25 96:23 143:7,10,11 148:9 154:14 165:25 166:5 209:15,22 230:19 252:14,16 252:17 261:2 technology-based 66:16 techsafety.org 40:18 teddy 53:18 tedious 171:9 195:18 tee 91:3 Teen 30:12 teenager 200:12 teens 26:19 tees 121:25 telecommunicatio... 147:23 Telegram 182:20 telephone 12:4 television 223:22 tell 59:22 91:11 94:25 114:21 115:1 131:10 150:25 155:16,18 164:8 188:15 189:13 218:4 222:14 273:15 telling 54:14 77:12 tells 221:5 ten 15:14 107:8 tend 73:19 147:6 171:2 218:12 230:6 263:7 tendency 149:3 265:14 tends 245:15 tens 31:21 259:2 tension 109:14 tent 121:12 122:23 tents 69:6 125:9 tenuous 77:3,3 term 7:4 17:10 71:22 119:10 215:1 termination 170:6 terms 23:22 24:7	51:12 54:1,2 59:8 81:17 82:20 88:12 92:16 98:10 100:22 113:12 129:18 152:22 171:22 210:14 218:13 226:9 228:17 230:12,22 247:3 263:13 266:13 270:13 272:8 274:10 275:6 277:12,13 terrible 175:21 272:9 275:11 test 18:12 45:16 70:22 71:2 76:11 76:14 82:5 85:5,8 85:14 86:6,8,13 93:6 95:1 155:8 tested 198:9 240:21 testing 45:20 103:14 104:14 tests 46:14 70:16 71:3 76:9,22 77:10 85:1 93:5 Texas 20:13 texts 260:23 thank 5:25 6:12,18 6:19 14:15,17 17:14,17 25:2 32:18,23 39:6 43:19 49:14,15 55:22 64:22 69:11 79:18 83:8 125:14 126:21 137:17 140:20 143:13 166:18 170:14 177:11 183:15 202:9 203:6 206:1 206:3 207:8,10 210:13 211:21,23 211:23 214:11,13 219:10 222:6 230:24 263:15 265:9 267:19 268:25 269:1,5 278:3,4,9,23 279:1 thanking 207:11	thanks 6:21 16:25 44:4 69:12,12 74:4 74:4 83:8,9 90:25 101:12 121:6 135:20 140:21 143:23 164:17 172:1 175:6 180:6 231:17 233:13 236:1 239:17 242:18 244:18 246:4 248:1 250:11 252:24 254:7 256:3 279:5 theft 11:19 13:3 17:10,12,13,19 18:15,18,20,20 19:20 20:23 21:4,8 21:25 22:1,2,19 23:23,24 24:1,3,12 24:25 25:5,7 50:2 50:14 59:12,19 65:2 120:13 158:7 211:3 212:10 214:7 215:2,22,23 216:3,10,17,18,21 217:2,8 231:25 232:16 243:1,25 245:10,15,21 246:3,21 251:1 252:9 253:8,19 256:10,15 257:7 257:19 258:2 266:13 267:3 theme 122:1 theoretical 109:1 267:22 theory 93:22 125:1 142:5 thhe 162:13 thickness 27:20 thief 18:3 thing 19:8,14 26:17 28:3 29:2,12 30:20 30:23 39:23 45:18 47:7 49:23 54:22 75:23 76:16,20 83:21 84:4 89:11 90:12 91:13 95:8
--	---	--	---	---

<p>95:11 98:8 99:1 106:7 121:23 124:4,21 126:25 129:11 130:3 132:2 138:1 139:14,25 166:23 168:3,7 170:9 201:14 203:24 206:7,16 217:19 217:25 218:25 230:13 242:4 243:25 257:5 260:25 261:11 262:17,22 263:8 263:12 264:2 265:13 266:12 267:8 271:10 273:13 275:4,11 277:19 278:17 things 16:9 22:16 23:1,21,22 25:25 26:1 28:11,23 30:11 31:8,18,23 32:5,8 35:11,12 40:22 41:21 42:2,8 42:10,16,25 43:4 43:17 47:4 49:11 51:2,4 53:5 54:24 56:24 57:2,3 58:14 61:1,3,4,12 64:6 66:15 75:19 77:23 83:13,17,19,23,24 83:25 84:10 87:5 87:24 88:4,15 89:5 90:7,12 92:18,22 94:6 96:21 98:7,17 103:10 104:4 105:6 108:16 109:17 111:12 115:5,10,18 116:10 126:18 136:12 139:16 145:18,23 146:5 146:18 151:25 152:16 153:6 156:24 157:20 159:3 163:8,14,25 164:11,13,25</p>	<p>165:22,24 169:8 170:1,2,3,5,7,13 170:20,25 174:6 178:3,8,16 181:3 183:24 184:2,10 184:13 191:16,20 192:4,5 194:11 197:17,18 202:3 203:17 204:9 205:4,6 214:8 216:2 217:18 221:20 226:11 228:4 232:4,5,13 233:9 234:14 235:23 242:3,14 242:22 244:21 246:7 247:2,18 250:7 255:22 258:4 259:16 262:8 263:1,6 268:19 271:5,7 272:24 275:25 think 12:15 17:17 17:18 28:22 30:24 33:1 35:18 36:2 37:11 39:22 40:12 40:14 41:11,22 42:10,25 49:22 50:1,2,3,3 51:2 55:12 57:5,18,18 57:21 58:9,25 59:25 60:3,6,22 61:7,8,19 62:6,12 62:20,21,24 63:12 63:20,23 64:17 65:17 66:1,16,24 70:6 71:18 72:12 74:9,24,25 75:8,12 75:18,20 76:9,11 77:3,5,14,15,23,24 79:7,9,12,25 80:4 80:18,19,21,24 81:5,7 82:11,13,20 82:22 84:22 85:21 85:23 86:11,14,20 87:7,9,12,13,14,16 87:19 89:6,12 90:12,12,13,15,18</p>	<p>90:23 91:3,5,6,12 91:14 92:2,3,11,12 93:13,18,20,21 94:8,10,12 95:7,7 95:19,25 96:20,25 97:2,2,23 98:2,11 98:19 99:2,3,8,15 99:17,19 100:6,6 100:10,19 101:2,9 101:13 102:4,10 102:11,12,25 103:1,6,6,9,15,20 104:8,10,21,24 105:18,21 107:23 109:25 110:3,7 111:11 112:14,19 112:20,21,23 113:16,24 114:2,3 114:16,16 115:2,4 115:9,18 116:23 117:23 118:14,16 121:16,17,23,23 121:24,24,25 122:5,6,22,25 123:12,13,16,25 124:23 125:7,15 125:18 126:20 127:3,9,11,11,15 127:18,19,20,21 128:1,4,9,9,11,24 129:2,14,19,23 130:1 132:1,2,5,13 132:17,18,19 134:9,17,21 135:15,16,23,25 136:2,2,11 137:20 138:3,6,7,19 139:1 139:4,7,15,17,19 139:21,23,24 140:2,4,5,13,15,17 140:18 144:3,6,16 145:12,14,17,20 145:21,23,24 146:10 148:7,15 149:14 150:9,17 150:21 151:2,9,11 152:10,11,18 153:8,18,18,23</p>	<p>154:4,24 155:10 155:14,16 156:7,7 156:8,11,16 157:5 157:8,12 158:2 159:16,23 160:11 160:14,18 161:4 162:5 163:14,15 163:21,21 164:6,9 164:10,10,20,23 164:25 165:18,20 165:25 166:2,5,16 166:21 167:12,15 167:17,21,25 168:4,11,18,19 170:21 171:3,10 172:3,6,10 173:1,3 173:18 177:13,15 177:19,25 178:12 179:15 180:16,17 180:18,18,20 181:7,9,10,15,16 181:24,25 182:2 182:24 183:21 184:18,18,25 185:15,23 187:7 188:18,19,21 189:10,20,20 193:23 194:13,17 195:15,23 196:3,5 196:12,17,22 197:10 199:4,7,21 200:7,21,25 201:3 202:10,15,23 203:1,9,12,18,24 204:8,16 205:10 206:12 208:6 212:3 214:9,25 215:20 216:2 217:1,13 220:4,13 220:13,20 221:12 222:8,10 225:13 225:14,16,17 226:8,9 231:4,13 232:2,5 233:9,10 233:13,20 234:3 234:14,21 235:10 235:16,17,21,23 236:4,10,11 240:1</p>	<p>241:17,17,20,23 242:11,12 243:22 244:14,25 245:18 245:19,20 246:3,7 246:18 247:4,14 247:18 248:5,15 249:19,19 250:5 252:14 253:20 254:9,13,17,21,25 255:12,18,24 256:5,9 257:5,15 257:24 258:3,3,25 258:25 259:9,14 259:23,25 260:3,8 261:13 262:8,15 262:22,23 263:13 263:16,17 264:1,3 264:17 265:13,15 265:22 266:3,9 267:20 268:11,21 268:22 272:7,17 273:7,9,22,25 274:1,6,7,8,19,25 275:14,22 276:13 276:22 277:21,22 278:8,18,21,25 thinking 10:18 37:8 57:24 58:13,23 72:1 75:10 83:14 89:3 104:23 123:16 124:1 135:2 146:11 150:21 160:1 180:12 219:12 221:6,8,21 231:19 232:23 259:13 262:1 264:4 272:19 273:3,5,23 thinks 113:18 146:8 247:16 third 7:16 13:18,24 78:7 79:6 112:7 130:19 144:1 180:25 224:19 238:8 251:9 274:17 third-party 224:21 Thomas 112:5</p>
--	--	---	--	---

<p>thoroughly 12:25 thought 37:18 46:9 90:9 138:12 174:13 193:15,21 217:7 229:24 244:24 268:2 271:11 272:24 thoughts 64:2,23 127:11 180:10 201:10 205:25 230:25 236:2 239:18 240:12,15 241:16 244:19 246:5 247:5 248:2 250:12 262:10 thousand 19:10 thousands 258:9 259:2 threat 142:25 192:15 238:11 threatened 50:5,6 54:8 threats 12:9 32:5 three 7:10 8:16 18:12 40:6 41:3 44:20 46:14 59:17 74:8 75:17 82:4 111:17,22 117:9 117:12 167:14 176:18 191:17,24 193:13 204:12 218:4 223:25 238:14 three-quarters 41:4 threshold 100:4 thrilled 143:25 throw 130:6 184:15 thrown 48:24 122:14 127:6,7 tickets 43:15,16 tie 95:2 110:5 133:9 214:8 246:11 251:17 253:7 tied 59:11 94:20 116:24 ties 82:23 99:17 203:25 time 5:13 6:1 17:5</p>	<p>46:22 49:25 50:11 60:4,7,19 65:22 76:17,19 80:14,15 84:7 87:5 90:21 105:17 110:4 111:2 116:1,15 117:2,2,12,20,20 118:17 120:3,5,7,8 127:21 128:7,18 130:4 137:3 139:3 139:4 146:11 156:23 167:13 181:3 185:11 187:3 190:17 193:1 197:15,16 200:7 202:2 205:4 205:12,21,21 206:14 212:11 213:11 215:12 217:6 219:14 221:10 233:8 234:20 243:8 244:3 245:15 247:2 250:7 254:18 258:11,14 258:21 260:23 263:24 266:13,19 267:1,6 269:1 270:4,25 276:15 277:15 278:4 279:1 timely 8:8 times 25:19 29:4,4,6 45:2 107:8 117:21 124:19 134:9 158:17 184:7 187:10 208:6 231:11 237:4 246:17 timing 17:17 Tina 192:18 tiny 39:22 tire 8:9 199:5 tired 206:25 tires 43:17 Title 56:10 today 3:9 5:14 6:1,3 6:6 7:20 10:25</p>	<p>11:2 12:23 13:5 15:6 17:3,9,15 18:17 19:19 32:24 33:12 35:21 44:21 67:6 90:16 94:17 135:14 143:14 147:25 148:14 184:17 186:14 188:16 201:16 203:2 205:5 208:9 214:13 215:21 216:5 217:14 246:17 266:4 271:3 276:19 today's 3:12 5:22 6:18 15:2 token 101:21 told 54:6,7 toll 246:22 Tom 10:5 tomorrow 135:14 tons 206:9 tool 8:18 12:18 67:7 112:6 134:13,18 190:10 191:2 tools 61:13 179:7,16 190:21 191:21 192:14 193:7,17 199:3 201:6 202:4 202:7 top 88:13 163:18,24 175:17 181:24 216:10 252:2 270:21 top-level 57:21 topic 17:17 34:19,21 35:24 38:3 183:16 205:11 240:12 242:19 263:17 267:20 topics 7:2 9:15 25:5 208:19 266:8 271:2 Toronto 190:9 Toronto's 207:4 tort 94:2,7 121:18 122:10,16 127:2,2 127:6 135:11</p>	<p>205:6 267:12 totally 89:17 126:18 133:11 154:7 185:5 259:24 touch 8:6 175:8 176:12 177:12 185:22 touched 49:18 264:2 267:8,9 276:21 touches 181:4 touching 42:9 towed 256:22 town 53:11 trace 96:4 213:14 219:16 255:23 traceable 212:18 traced 213:3 262:2 track 70:15 93:4 184:1 201:2 251:22 252:16,17 266:19 267:7 trackability 252:15 tracked 72:23 tracking 70:12 71:22 73:7 80:6,13 80:23 81:11,17 93:7 96:22 99:11 105:6 120:10 trade 1:1 3:6 29:24 144:21 trade-off 235:19 trade-offs 7:18 218:2 trademark 142:4 trading 172:5,7 traditional 17:12 135:11 227:24,25 traffic 159:16,18 training 47:20 Trans 47:19 transaction 81:1 89:22 167:5 168:6 184:4 197:12 212:10 224:8 225:7,9 226:18 227:25 228:1 272:11 transactions 89:22</p>	<p>131:7 184:16 197:13 200:25 248:7 252:8 272:3 transcribed 280:9 transfer 219:6 transgender 47:16 47:19 52:18,23,25 transit 160:20 transition 170:15 250:13 transitional 41:17 translatable 244:13 translate 240:19 transparency 63:22 143:8 166:22 201:25 202:7 transparent 53:24 trap 96:4 186:16 trash 39:12 trashed 39:17 traumatic 51:24 travel 145:8 tread 95:5 treat 24:3 52:16 224:10 treated 48:9 198:12 267:25 treatment 19:9 43:6 treatments 19:8 trends 267:7 tricky 242:13 tried 30:21 35:24 87:7 92:4 97:18 202:3 220:7 237:23 249:12 273:2,4 tries 30:10 trigger 99:22 113:2 113:3 triggers 28:17 81:16 trivial 10:1 trojan 29:20 trojans 30:1,2 true 43:6 77:8 78:10 78:11,12 85:3 96:25 113:20 114:1 132:25 214:22 216:20,21</p>
---	---	--	---	---

234:9 242:11
 272:2 273:14
truly 78:3
trust 132:25 149:17
 152:18,18,22
 153:1 160:2 163:8
 182:3,5,7 183:4
 192:8
truth 223:7
truthful 79:2,7
 105:19 107:2,13
try 27:23 28:22 34:9
 34:20 36:2 39:2
 51:20 56:25 57:2
 91:18 92:13
 102:20,21 107:23
 116:23 117:18
 135:17 145:21
 146:10,14 152:17
 161:25 165:7,9,11
 165:15 166:10
 173:20 175:23
 176:4 179:11
 182:1 197:25
 198:9,23 199:8
 206:17 210:21
 211:18 213:8
 219:6 238:6
 242:21 245:9,21
 247:6 252:21
 253:7,17 261:6
 262:25 263:1
 265:14,20 266:10
 276:7
trying 26:3 43:8
 53:16 65:12 66:2
 92:3 97:17 98:10
 106:6 117:10
 123:20 136:24
 147:5 166:11,15
 188:19,25 189:12
 189:21 202:12
 208:8 210:10
 211:2 218:3 219:8
 219:16 220:18
 221:4,18 222:9,9
 228:10 234:11
 235:7,14 238:6

240:1 243:11
 245:10 254:14
 255:12,18 260:6
 260:23 264:1
 265:24 267:6
 268:24
Tucker 168:20
 209:12 217:15,15
 228:23 229:1
 240:17 244:24
 254:9 260:20
 265:11
TUESDAY 1:9
tugboat 227:9
turbocharge 36:13
turn 4:22 69:10
 161:16 242:16
turns 256:21 260:4
TV 187:19,21
TVs 187:21
tweet 5:23 39:13
 237:2,3,7
tweeting 5:21
twenties 26:20
twice 268:17
twisted 131:5
Twitter 5:21,23 54:9
 141:23
two 3:14 9:18 12:14
 22:23 23:8,11
 26:14 27:8,8 59:17
 60:8 74:7 76:6
 77:23 79:14 88:6
 89:5 93:3 94:15
 95:2 96:16,18 99:4
 105:21 107:6
 110:5,14 112:2
 113:1 124:9
 129:12 130:10
 136:3 139:11,21
 147:16 156:11,13
 158:10 167:14
 185:6 186:25
 194:11,18 209:10
 210:15 212:7
 214:15 217:18
 222:23 223:1
 228:20 240:10

251:15 255:1,4
 276:22
two-thirds 36:15
tying 129:11
type 13:11 28:24
 42:8 51:5 57:7,15
 59:4 63:9 103:1,2
 129:25 130:25
 131:2 166:12
 193:9 195:19
 215:23 216:12
 223:2 248:16
 259:11
types 7:7,12,22
 11:17 16:23 17:13
 22:18 33:6 36:3,9
 36:12 39:8 43:17
 49:11,17,20 56:20
 65:16 66:15,18,21
 132:8 145:21
 152:4 165:22
 219:12 220:3,5,21
 221:19,21 222:4
 225:1 234:5
 241:20 242:2,17
 244:2,2 255:13,20
 264:15 266:21
typewriting 280:6
typical 218:5 230:14
typically 19:7 80:10
 148:6
typologies 119:17

U

U.S 8:9 19:22 20:24
 30:19 200:22
 209:9 214:16
 215:4
Uber 8:15 162:17
Uber's 162:25
UC 222:20
ultimate 7:20
ultimately 122:5
 123:20
unable 21:16
unambiguous 23:9
unauthorized 7:23
 15:4 110:12,14,17

110:19,23 112:13
 112:18 113:5
 114:20,23,24
 116:6 211:7
uncertainty 249:4
 250:6
unclear 75:22
 122:16 123:5
unclick 184:22
uncovering 223:7
underdeveloped
 254:25
undergo 45:16
undergraduate
 229:9
undergraduates
 229:19 230:18
underground 26:16
 29:22
underlying 159:14
 188:15
undermine 137:15
underpolicing 51:13
understand 5:19
 7:16 10:2,11 13:9
 29:14 32:13 36:3
 46:12 51:3 54:23
 57:6 63:21 66:2,21
 75:24 83:17 84:9
 84:10 85:22 86:22
 88:11 93:13
 112:15,16 134:23
 152:17 153:3,19
 154:11 162:1
 165:15,16 166:3
 167:16,24 171:10
 172:6 173:4 177:8
 180:19 182:7
 185:7,24 186:4,7
 191:21 194:13,16
 194:19,20 208:11
 220:5 221:4,18,19
 222:10 230:19
 235:14 242:22
 250:24 255:12,19
 256:6,6,7,8 265:21
 265:24 271:16
 273:10

understanding
 13:25 50:24 51:5
 52:23 55:13 59:8
 67:5 81:2 99:10
 166:11 168:12
 171:3,5 172:4,14
 173:6,8,13,17
 174:7 175:1
 181:10 197:8
 234:5 235:18
 247:5 254:12,15
 270:16 278:6
understands 181:4
understood 89:12
 225:5 267:21
 277:14
undertake 164:2
undertook 57:6
unethical 59:12
unexpected 95:12
 95:22
unfair 8:20 36:22
 112:8 236:11
unfairly 268:15
unfairness 10:17,22
 10:24 11:3 37:7
 112:6 128:9,10
 129:3 135:16
unfettered 138:5
unfortunately 17:9
 19:17 22:8 23:9
 28:21 29:22 42:5
 188:25 198:14
 200:15 250:10
 253:20 269:1
 270:25
unfounded 94:18
unhealthy 40:3
unimportant 223:14
unintended 9:23
 62:22 218:5,7,15
 219:1
Union 143:9 173:20
 174:3 206:15
Union's 143:5
Union/Consumer
 187:14
unique 6:25 19:4,21

24:25 30:18
 190:20
Unit 209:5
unite 104:11
United 1:1 21:3
 138:8 151:9
University 68:13
 142:3 190:9 207:4
 208:23
unknown 151:15
 172:12
unlock 213:9
unpack 91:1
unrealized 273:18
unreported 214:19
 215:2
unsecure 183:6
unsecured 199:23
unsure 179:25
untenable 109:12
 121:5
unuseful 89:17
unwarranted 13:4
update 123:25
 223:18
updating 123:14
 124:3
upside 272:15
urged 88:14
urgency 94:9
USA 30:12
usage 167:22
use 3:18 4:4 7:20
 10:9,12 23:6 31:13
 31:13 32:1 35:20
 37:4 41:7 47:15
 48:3 51:4 52:7
 54:19 55:19 57:16
 63:2 79:10,11
 97:25 105:25
 107:15 119:21
 121:2 144:5
 145:25 146:3,9,16
 147:4 150:21
 151:4 152:11,21
 152:22 156:8
 157:7 159:16
 160:17 161:3,20

166:10,13 172:8
 172:24 173:23
 175:22,23,24
 179:9,12 185:9
 186:9 187:20
 189:5 190:14,23
 202:19 203:12,13
 204:2,14,24,24
 206:19 209:15
 211:13 217:21
 220:20 221:5
 224:18 225:25
 226:1 229:22,23
 229:23 230:15,16
 234:25 244:15
 248:20 254:4
 255:5 274:24
useful 95:7 106:10
 109:21 157:25
 228:16
user 104:13,14
 132:8 175:21
 186:25 251:24
users 145:8 172:22
 176:1 187:9
uses 12:16 33:14
 70:12,19,24
 104:22 105:20
 162:9 203:19
 275:16
usually 18:21 99:3
 169:22 181:21
 193:1 258:7,10
 264:10
Utah 18:1,7,25
utility 74:19 83:20
 89:13 90:5 101:23
 103:11 104:15
 211:5,14
utmost 115:14

V

Valdez 226:22,22
 256:18,19,24
valid 123:2 186:10
 268:20
Valley 166:7
valuable 14:10

103:25 144:13
 156:22 161:16
 266:1
valuation 223:1
 226:13,21 227:6
value 88:8 131:20
 144:12 147:15
 158:1,7 168:21
 169:4 176:1
 210:22 211:2,5,10
 211:11,13 221:4
 222:10,12,17,23
 223:14 224:24
 225:20 226:10,10
 227:13 234:20
 235:17,23 238:1
 249:8,13 257:2,3
 258:1 261:14
valued 104:13,14
 235:3
values 138:11
vandalized 49:9
variable 158:11
variation 260:24
varied 15:7
varies 196:6
variety 65:16
 240:24 271:22
 274:17
various 10:12 15:9
 16:23 17:18 18:22
 84:2 159:25
 160:10 203:14,19
vary 149:14 154:7
 157:13,14 245:16
varying 204:17
vast 137:2,3,3
vehicle 253:19
vendor 24:18
verification 161:25
verify 162:4
version 184:12
versus 62:3 104:3
 112:15 148:23
 195:11 220:25
 257:16 274:22
 275:1,18
vexatious 94:5

viable 98:13
vibrant 146:15
vice 16:11 142:13
victim 19:13 30:1,11
 40:23 41:9 42:1,5
 42:18,20,23 43:7
 51:17 53:7,10
 196:20 213:6
 215:14
victim's 18:9 29:20
 31:8 41:23 43:12
victimization 40:13
 209:5,9 214:15
 215:13,14,15,17
 216:8 243:10
 266:6
victimizations 215:7
 216:7
victimizing 19:25
victims 12:10 18:15
 19:16 23:23,25
 25:24 26:4,13,18
 26:19 29:18,25
 30:9,15 39:8 40:22
 41:15 43:1 53:15
 54:1 59:18 65:16
 216:7,9,10,21,22
 217:2,8,13 244:16
 253:13,14,25
victims' 19:9 31:23
video 26:15 29:10
 73:7,7,8 223:16,18
 224:12 236:16,18
 236:22,25 237:11
 237:14,24 248:25
 249:9
view 33:1 111:23
 123:17,18 168:4,5
 168:7,19 198:16
 212:24
viewing 141:22
 224:16,17
viewpoint 257:1
vigilance 262:6
vigilant 96:25
VII 56:10
vindicate 96:15
violates 95:23,23

138:15
violation 80:1 95:20
 96:3 112:2,3
 129:21
violations 13:11
 81:7 116:8 130:9
 130:11 132:18
 208:20
violence 16:12 31:16
 31:17 39:8,17,21
 39:21 40:20 41:14
 42:16,20 43:7
 50:13 53:7,15
 62:17 64:12
violent 215:18
viral 262:20 263:6
virtual 179:19
vis-à-vis 140:3,3
visited 30:18 90:20
 272:12
volume 33:2 234:8
VP 164:7
vulnerabilities
 191:20
vulnerability 110:11
 123:23
vulnerable 34:8
 112:9 183:2

W

wait 205:6
waiting 257:21
waivers 184:20
walk 80:4 90:11
walking 72:22 121:7
wallet 240:23 241:1
 241:3
wallets 240:24 241:6
wand 90:3
want 4:5 5:25 14:3
 17:7 21:24 23:22
 37:3,10 44:18
 46:13,16,16,17
 49:3,10 52:16 54:8
 55:5,8,20 61:13,21
 64:4 66:18 67:19
 68:7,15 69:5,25
 72:10 74:10,15

75:3,3,5 80:18	113:13 121:10,11	111:24 112:22,22	98:20 101:13,15	wearing 47:4
82:25 83:11 84:20	130:6 133:15	113:18 116:19	101:15,18 103:2	web 110:20 111:13
86:17 87:20 91:17	175:8 176:12	123:15 127:13,15	104:22,24 105:3,9	113:22 123:9,10
92:10 93:24 95:15	178:21,24 180:7,9	127:21 129:2	105:12 106:4	123:10 172:22
96:13 97:4,10	183:24 185:9	132:5,23 133:20	111:20 115:4,7,18	245:7 251:22,23
98:25 102:17	201:22 206:6	135:18 159:15,19	117:24 123:20	252:12
103:23 104:11,20	207:3 240:23	167:1,9 169:2,10	126:9,11 136:1	webcast 5:3,10,10
105:24 107:4,13	261:6	174:25 179:11	137:12 145:3	141:22
113:9 114:15	wanting 187:19	180:3,5 184:13	147:20,25 150:16	website 12:8,12
115:15 116:16	wants 91:3 98:9	191:10 192:20	160:19,22 161:4	117:10 165:11,15
119:8 122:23	warn 115:24	198:7 202:19,20	162:21,24 163:10	175:14 182:4
126:25 127:10,12	warning 198:13	213:13 217:17	167:2 171:14	183:25 184:23
127:20 129:5,8	warped 134:7	221:21 224:5	175:16 186:14	235:5 278:11
135:13 137:13	warranty 167:9	225:4,14 227:5	187:24 188:18,19	websites 55:4 145:9
140:15 146:19,23	170:6	230:7 231:22	188:25 189:12,17	194:24,25
154:21 156:6	Warren 117:8,9	235:9 236:11	189:18,21 195:12	week 117:1 173:15
157:22 158:5	washing 248:22,23	240:4,7,19 241:24	196:6 199:17	268:6,8
160:15 164:17	Washington 1:15	242:16,22 247:25	204:8 206:13	weeks 26:8
167:18 168:3,19	143:6	250:18 252:5	214:20 218:9	weigh 7:17 10:3
172:17,18,21,25	wasn't 51:23 75:24	257:25 262:24	221:14,20 224:7	13:19,22 144:14
173:1 174:5,25	117:11 127:3	265:5 269:3 272:2	225:23 228:2	170:16 180:10
175:2,10,19,20,21	150:22	272:6	231:22 240:11	weighed 146:3
178:23 179:5	waste 120:7	ways 24:21 35:17	241:25 242:25	weighing 144:5
180:14 184:12,12	wasted 117:12	50:7 54:11 58:18	246:13 247:15	160:11 202:23
185:12 187:6,10	wasteful 105:24	58:21 63:19 78:20	248:4 254:14,17	weights 182:9 200:12
188:3 190:21	watch 158:21	83:18 87:15 100:6	255:21 259:2,19	weight 264:23
194:12,13,16,20	159:21,21 189:24	128:5 134:18	260:10 261:22	weird 49:7
194:20 195:19	193:11 236:19	135:4,7 138:16	266:20 267:5	welcome 3:5,7 5:9
197:1,6,7,9,11,22	watched 237:4	159:3,14 163:3	268:23 271:12	6:13 141:6 208:4
197:24 200:14	watching 5:9 23:19	166:16 167:22	273:5,10 276:12	213:9
201:18,21 202:17	159:18 192:10	180:3,20 182:17	276:14,24 277:4	welfare 9:21
204:10,12,13	237:6	190:25 198:23	we've 24:23 35:8,17	well-intentioned
206:15,19 212:7	water 4:10 275:3	199:8 209:2 220:7	50:4,9,11 64:10	51:19
213:17 214:4	waters 271:21	221:19 234:7	83:24 115:5 130:3	well-paying 54:20
218:7,16,25 224:4	wave 90:4	241:12,21 247:5	146:6 152:16	went 18:6 48:17,22
228:14,21 231:1	waving 279:4	247:20 253:6	159:25 162:15	48:23 73:10 74:7
234:23 238:19	way 17:22 20:21	255:18 259:13	175:15 183:16	80:14 101:14
239:19 241:7	22:16 24:14 29:16	266:5	186:19,21 195:14	111:10 116:4
245:2 250:25	34:16 39:4 42:1	we'll 111:1 189:25	196:22 198:21	185:24 227:6
251:1,3,8,12,13,15	43:10 52:9 53:19	194:15 200:8	200:23 210:24	238:16
259:12,21,24	54:14 56:13 57:4	224:15	219:1 253:5	weren't 176:23
260:9,15 261:16	61:23 62:19 63:7	we're 5:9 15:11 48:3	261:17	193:19 237:13
262:13,23,25	70:13 80:1 81:6	51:2,5,8 57:23	weak 71:7	what-all 171:10
264:12,13 265:1	84:14 88:13 90:24	58:13,23 63:23	weakness 225:6	whatnot 275:18
266:8,9,10 268:23	91:11 92:23 95:12	65:12 66:8 67:2	weaknesses 223:3	whatsoever 166:24
271:3 275:2,4,8,9	95:22 96:9 102:22	68:24 70:1 75:9,10	225:18 228:1	217:4
278:3,3,6,23 279:1	105:2 107:8,14,23	87:13 90:16 93:24	wealth 108:5,12	white 34:11 214:24
wanted 39:10 47:2	108:10 109:19	95:4,11 97:22 98:6	259:5	Whitman-Walker

16:16 44:6 53:2
wholly 37:23
Wicker 182:20
 183:14
wide 9:1 15:6 49:16
 148:12
widely 95:8 225:5,5
widespread 195:13
 265:7
WIFI 191:19
wildly 202:15
William 226:24
 228:7,9 256:18
willing 74:15 97:15
 126:14 222:2,5
 231:6 235:13,24
 236:13 238:9,20
 238:22,24 239:2
 259:25 260:4,7
 273:20 274:2
willingness 225:23
 225:25 232:18
wind 34:17,25
 263:10
window 48:17,19
 250:1
winds 239:10
winners 108:4,9
wiretap 96:9
wisdom 96:5 135:9
wish 22:3 25:16
 33:22 60:16 90:3
 201:1
wishful 262:1
withdrawal 45:24
Wolff 209:19 219:10
 233:20 235:21
 241:17 246:7
 254:21 258:3,25
 264:1
woman 17:25 18:6
 18:25
women 39:25 40:4
women's 47:23 48:3
wonder 232:8
 258:17
wonderful 15:12
 208:10,13 245:20

265:12 269:3
wondering 49:5
 52:5 228:24 230:4
Wood 3:15 6:22
 15:2 49:14 60:5
 61:24 63:25 64:22
 67:11,18 143:15
 146:17,25 148:24
 149:10 150:13
 153:10,16 154:19
 155:14 156:3
 157:9 158:12
 159:25 160:10
 162:11 163:11
 164:16 173:24
 183:16 185:4
 186:17 188:2
 190:4 191:12
 193:23 195:8,22
 196:23 198:18
 200:7 201:7 279:5
word 87:14 89:7
 137:18 138:2
 152:24 202:25
 206:2 261:5
words 20:10 49:8
 80:14 93:17
 112:18 115:3
 200:9 201:15
 229:22,23 239:21
 248:4
work 6:2,4 7:21
 8:13 14:10 20:4
 22:16 24:9,24
 34:10,18 42:7 45:4
 46:8,25 47:2,7
 50:15 52:5 54:22
 56:7 64:11 72:12
 98:19 107:24,25
 108:22 139:22
 140:8 143:6
 161:23 167:1
 168:21,24 173:10
 175:15 179:22
 181:1 182:18
 190:2 196:22
 198:9 202:5 210:3
 210:10 211:9

222:16 224:7
 228:23 229:3
 243:15 245:9
 252:22 255:20
 258:12 263:22
 271:13 272:9
 273:9 274:25
worked 6:20 18:1,18
 46:3,20 47:17
 155:17 163:1
 219:11
worker 40:10 46:21
working 18:13,22
 24:7,10 34:14
 49:25 59:15 64:19
 87:9 139:3 147:23
 166:8 205:23
 210:8,15,21
workplace 38:10
 44:21,24,25 45:5
works 20:4 163:18
 222:15
workshop 1:6 3:8,19
 3:23 5:11,22 6:19
 6:21 7:10 8:8 9:17
 11:5 14:11 15:2
 16:22 17:16 34:19
 50:15 98:18
 109:21 130:25
 131:1 134:21
 202:11 245:4
 278:25 279:7
world 9:3 15:23
 30:20 51:25 54:15
 65:21 100:13
 116:20,21 117:5
 122:7 123:18
 133:25 138:4
 142:20 171:7
 182:15 183:22
 185:2 235:4
 265:20 277:5
world's 118:5,6,7
worldwide 157:20
worried 52:15 95:13
 106:4 117:17
 213:17
worry 144:23

198:11 202:6,6
 213:6 265:19
worse 87:10 100:18
 170:5 240:18
 263:12
worst 31:15
worth 10:19 38:15
wouldn't 79:3 164:5
 248:6 249:1
wow 270:21
wrap 111:6 170:8
wrestled 253:5
writ 57:24 66:25
write 50:12 123:6
 135:12 238:25
writes 142:6
writing 88:14 89:12
 203:20
written 59:14 78:1
 121:9 262:25
wrong 76:1 136:23
 139:12 150:25
 174:9 188:11
 273:16
wrote 49:8 135:15
Wydra 16:15 44:4
 52:10 56:6 66:10
Wyndham 11:18

X

Y

Yahoo 162:17
yeah 44:4 47:7
 52:10 62:10 71:20
 74:4 76:3 89:20
 111:10 118:2
 121:11 123:7,7
 138:3 139:12
 151:11 156:6,14
 163:13 164:23
 166:20 170:19
 175:8 177:11
 178:18,24 179:2
 181:8 182:11
 185:5 202:9
 222:16 231:1
 236:4 239:19

240:17 250:20
year 108:25 120:20
 123:5 164:4
 169:12 174:20
 179:10 190:1
 192:9,12,19 215:9
 220:12,17 225:13
 227:8 251:23
 256:11 257:9
year's 102:3
years 7:9 35:2,12
 40:18 41:3 42:11
 47:22 59:17 64:11
 64:12 88:14 98:19
 120:19 142:16
 158:8,10 159:9
 162:16 167:14
 171:8 185:16
 186:1 191:17
 193:13 215:22
 222:19 238:14
 255:4 271:14
Yep 140:20
yesterday 190:9,19
 237:2
York 20:15 107:9
 238:16
young 20:1 26:18
 32:7
younger 26:22

Z

zero 89:16 126:12
 126:13 174:14,23
 212:17
Zigbee 191:19
zones 21:20

0

1

1 2:9 15:1 20:18
 124:12 126:17
 169:19
1.9 251:24
1/2 222:19
1:46 141:2
10 22:20 159:10

236:16,24 237:9
 237:22 249:8,11
100 65:8 113:21
 229:11 245:15
 271:14
101 2:9 15:1 47:19
11 25:17
11-year 142:12
11:00 4:8 67:14,16
 67:18
11:15 67:14,20
11:30 4:8
12 1:9 26:2,8 215:6
 216:14
12-year-old 51:17
12:46 140:24
120,000 19:11
13 27:2
14 28:7
141 2:14
15 2:9 29:16 80:15
150 113:21
16 30:7
17 30:23 40:18
18 35:23 40:7
 107:10 237:4
19 40:5
190 174:12
1934 147:24
1970s 214:16

2

2 2:11 68:1
2.5 124:20
20 158:8 169:5,11
 176:3,3 216:21
 252:2 253:24
 256:11,21,24
200 59:23
200,000 215:8
2000 40:20
20024 1:15
2014 39:17 40:19,23
 229:11
2015 142:12 208:24
2016 21:6 143:9
 209:1 211:25
 267:3

2017 1:9 20:21
 208:24 209:1
2018 267:5 278:15
2019 278:17,22
208 2:17
21 70:11
22 110:8
24-hour 41:16
25 106:15 107:11
 194:9
26th 278:9,10
27 64:11
270 2:19
28th 278:15

3

3 2:3,14 124:12,19
 126:17 141:3
 222:19
3:00 4:9
3:30 207:14
30 217:9 232:14
 253:14 254:3
30-minute 67:13
3000 169:12
34 111:5

4

4 2:17 208:1
4:45 270:5
4:58 279:7
40 142:16 232:15
400-7TH 1:14
41,000 41:16,18
44 192:24
45-day 278:7
45,000 228:10

5

5 8:19 9:11 10:24
 70:2,5 136:19
 145:17 232:20
50 204:10
50,000 228:8
500 8:12
5000 190:20
57 237:3

6

6 2:6 20:5
600 191:17
6000 26:7,8,23
68 2:11

7

7 20:20
71 41:4
72,000 41:15
76 232:8
7th 4:22,23

8

8 21:5 169:17
8,000 256:11

9

9 21:14
9:15 1:10 3:3
911 28:15
97 40:23