Weaving a Tapestry to Protect
Privacy and Competition in the Age of Big Data

Julie Brill
Commissioner, U.S. Federal Trade Commission

Presented at the European Data Protection Supervisor's
Workshop on Privacy, Consumer Protection and Competition in the Digital Age

June 2, 2014

Good morning and many thanks to the EDPS for inviting me to speak to you today about consumer protection, competition, big data, and the Internet of things.

Depending on whom you ask, big data algorithms – and the proliferating pipelines of connected devices through which we feed them – are either the beginning of a wondrous future, or the end of the world. Smart cars apply brakes before we sense danger; smart cars tell our insurance company when we shoot a red light. Big data analytics predict where flu will hit next and which newborns need early intervention; big data analytics suggest we might not be the best person for that new job or fit in at the local country club.

One cannot help but recall those famous opening lines from Charles Dickens's *Tale of Two Cities*: "It was the best of times, it was the worst of times, it was the age of wisdom, it was the age of foolishness…."[1] Even today, there is Manichean comfort in seeing the world in black and white – especially events as messy and earthshattering as revolutions, be they French or cyber. But that would be a mistake, especially for those of us charged with protecting consumers and competition in an era of rapid technological change.

I am particularly loath to belly up to the binary when it comes to choosing our tools for protecting privacy. Some, like Sun Microsystems' former CEO Scott McNealy, say that even that is a false promise – that privacy itself is a concept that has already faded to black.[2]

Others recognize some possibility of privacy in the era of big data but argue that several longstanding Fair Information Practice Principles are no longer of use. In particular, this crowd advocates privacy protection regimes that focus on limiting or stopping harmful uses of data.[3]

---

[1] CHARLES DICKENS, A TALE OF TWO CITIES 1 (A. B. de Mille ed., Allyn & Bacon 1922) (1859).

[2] McNealy was quoted as saying to a group of reporters and analysts: "You have zero privacy anyway. Get over it." *See* Polly Sprenger, *Sun on Privacy: "Get over It"*, WIRED (Jan. 26, 1999), *available at* http://archive.wired.com/politics/law/news/1999/01/17538.

[3] Craig Mundie, *Privacy Pragmatism: Focus on Data Use, Not Collection*, FOREIGN AFFAIRS (Mar./Apr. 2014), *available at* http://www.foreignaffairs.com/articles/140741/craig-mundie/privacy-pragmatism (arguing that "the era of 'big data, . . . has rendered obsolete the current approach to protecting individual privacy and civil liberties" and that regulators and lawmakers should "shift[] the focus from limiting the collection and retention of data to controlling data at the most important point – the moment when it is used") [hereinafter Mundie, *Privacy Pragmatism*]; FRED H. CATE, PETER CULLEN & VIKTOR MEYER-SCHÖNBERGER, DATA PROTECTION PRINCIPLES FOR THE 21STCENTURY: REVISING THE 1980 OECD GUIDELINES 10 (2013), *available at* http://www.microsoft.com/en-

Other principles – such as providing robust, meaningful notice, and data minimization – have at most a small role to play in this approach.

Use- and risk-based regulatory approaches are important, even necessary, but they are not sufficient. They don't cover all the droplets of small data – much of it from interactions consumers have with their favorite online retailers, social media sites, and apps – that flow in surprising ways, out of context of the original interaction, into the rivers of big data. I am not suggesting we ignore the practical realities of big data. I am suggesting that we must get creative – stop asking *whether* proven tools like notice, choice and collection minimization apply in a big data era and ask instead *how* we will apply them.

When it comes to the challenges faced by consumer privacy in this cyber-century, we ought not to be thinking "either-or" but rather "and". We ought not to search for a single thread, black or white, that will tie up all our privacy concerns, but instead weave a rich tapestry, made colorful and strong by the warp and weft of regulatory approaches old and new to the collection and use of consumer data.

Today, the quantity of personal information sucked into the cyber-vortex is growing exponentially. 1.8 trillion gigabytes of data were created in the year 2011 alone – that's equivalent to every U.S. citizen writing three tweets per minute for almost 27,000 years.[4] And it's predicted that the total amount of data will double every two years from here on out[5] – a churning that has required some scientists to experiment with immersing their servers in mineral oil to keep them from melting down.

Perhaps more important than the rapid growth in available data is the proliferation of data sources. Networking giant Cisco estimates that there will be 25 billion devices connected to the Internet by 2015.[6] By 2020, there could be as many as 40-50 billion.[7] By the end of this decade, 40 percent of data floating in cyberspace will come from sensors in our homes, cars, and other gadgets.

Some cars today have more than 100 computers in the vehicle, and manufacturers will soon make it standard for autos to run apps and access the Internet over 4G networks. And before we know it, our connected homes will turn down the heat for us after we've gone to work and turn off that kitchen light we forgot when we went to bed.

---

us/download/details.aspx?id=41191 [hereinafter CATE ET AL., DATA PROTECTION PRINCIPLES FOR THE 21ST CENTURY].

[4] Lucas Mearian, *World's data will grow by 50X in next decade, IDC study predicts*, COMPUTERWORLD, June 28, 2011, *available at* http://www.computerworld.com/s/ article/9217988/ World_ s_data _will_grow _by_50X_in_next_decade_IDC_study_predicts?pageNumber=1.

[5] Steve Lohr, *The Age of Big Data*, N.Y. TIMES, Feb. 11, 2012, *available at* http://www.nytimes.com/2012/02/12/sunday-review/big-datas-impact-in-the-world.html?pagewanted=all&_r=0.

[6] Cisco White Paper, *The Internet of Things, How the Next Evolution of the Internet is Changing Everything,* at 3 (Apr. 2011).

[7] *Id.*

Convenience is only part of the story. Scientists, entrepreneurs, academics, and policy makers see the potential for all this big data to fuel solutions to important social challenges, from reducing the amount of gas we waste sitting in traffic jams and more efficiently managing our energy consumption to achieving breakthroughs in healthcare.

But many also see risks to consumers in these vast storehouses of data. They could become fair game for data brokers – large firms unknown to most consumers, operating in the cyber shadows – to collect and combine into profiles of each of us. When run through their big data mill, even these innocuous bits of data can predict sensitive personal behaviour and characteristics – where we live, where we work, our daily activities, as well as our race, our financial status, and our health conditions. Data brokers may infer we are "Financially Challenged" or perhaps have a "Bible Lifestyle."[8] They may place us in a category of "Diabetes Interest" or "Smoker in Household."[9] Some of them sell marketing lists that identify consumers with addictions and AIDS. Others focus on ethnicity and finances, creating consumer lists such as "Metro Parents" (single parents who are "primarily high school or vocationally educated" and are handling the "stresses of urban life on a small budget") and "Timeless Traditions" (immigrants who "speak[] some English, but generally prefer[] Spanish").[10]

Data brokers mine the mountain of data generated about individual consumers and create the gold their clients turn to cash by sending us advertisements we might be interested in, an activity that can benefit both the advertiser and the consumer. But these profiles can also be used to determine whether and on what terms companies should do business with us and could result in our being treated differently based on characteristics such as our race, income, or sexual orientation.

The Internet of Things will exponentially expand the deeply personal information that is the data broker's fodder. Connected devices will offer a detailed view into where we are, what's happening in our homes, and what our children are doing. And this data will be sensitive and difficult to deidentify. Smart grids will record when we go to bed at night and when we wake up in the morning. Connected refrigerators will monitor what we eat and drink. Wearable devices will track our weight gain in real time.

Outside the Scott McNealys of the world, not many dispute that consumer protection, particularly consumer *privacy* protection, needs to be rethought and reinvigorated in the face of burgeoning big data and the connected devices that will feed it. A few weeks ago, in the U.S., the White House released a report discussing how we might embrace the good that can come from big data technologies without sacrificing fundamental values like privacy, fairness, and self-determination.[11]

---

[8] FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 20 n.52, 21 (2014) [hereinafter DATA BROKER REPORT].

[9] *Id.* at 46, 55.

[10] *Id.* at 20 n.52.

[11] EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES (2014), *available at* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf; PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., BIG DATA: A TECHNOLOGICAL PERSPECTIVE (2014),

The report is particularly concerned about big data algorithms that data brokers or their clients could use to discriminate against consumers in ways not captured by our current system of fair credit, employment, housing, and other civil rights legislation. To address these and other issues, the White House report calls for new laws on data security, data breach notification, and baseline privacy rights. I applaud the Obama Administration for its strong agenda for action.

At the same time, the President's Council of Advisors on Science and Technology issued its own take on the future of privacy frameworks in the world of big data. This advisory group's report presents a dim view of notice and choice requirements, claiming that "only in some fantasy world do users actually read these notices and understand their implications before clicking to indicate their consent."[12] Some privacy scholars, both here in the EU and in the U.S., share that opinion and believe we should stop trying to provide notice of and consent to the collection and use of data and instead monitor its actual use (or misuse).[13]

Notice and Choice, Use Restrictions, and the Role of Competition

At my agency, the U.S. Federal Trade Commission, we try to take a more textured approach, one that is on full display in our work on data brokers. Just last week, the FTC published a study of the role played by data brokers in big data analytics. We looked at nine data brokers. The scope of the information collected by the data brokers touches virtually every U.S. consumer: One broker has amassed records about 'nearly all U.S. adults and households', and adds 3 billion records per month;[14] another broker has a database with information on 1.4 billion consumer transactions;[15] and yet another has 3,000 data points on nearly every U.S. consumer.[16]

Our report recommends an approach that encompasses both use restrictions for data brokers and their downstream clients as well as meaningful notice and choice solutions to be implemented by data brokers and their sources of information.[17] Since most consumers have never heard of data brokers, we call on Congress to enact legislation that would lay out their existence and activities at a centralized portal, a solution I have long advocated.[18] At this portal,

---

available at http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf [hereinafter PCAST, BIG DATA: A TECHNOLOGICAL PERSPECTIVE].

[12] PCAST, BIG DATA: A TECHNOLOGICAL PERSPECTIVE, *supra* note 11, at xi.

[13] *See* Mundie, *Privacy Pragmatism*, *supra* note 3; CATE ET AL., DATA PROTECTION PRINCIPLES FOR THE 21ST CENTURY, *supra* note 3, at 10.

[14] eBureau, eScores Data Sheet, at 1, a*vailable at* http://www.ebureau.com/sites/default/files/file/datasheets/ebureau_escore_datasheet.pdf (last visited May 30, 2014).

[15] DATA BROKER REPORT, *supra* note 8, at 8-9.

[16] *Id.* at 8.

[17] I have prepared a summary of the FTC's legislative recommendations, which is available at http://www.ftc.gov/public-statements/2014/05/supplement-statement-commissioner-brill-commissions-data-broker-report. .

[18] *See, e.g.*, Julie Brill, A Call to Arms: The Role of Technologists in Protecting Privacy in the Age of Big Data (Oct. 23, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/call-arms-role-technologists-protecting-privacy-age-big-data/131023nyupolysloanlecture.pdf; Julie Brill, Reclaim Your Name – Keynote Address to the 23rd Computers, Freedom, and Privacy Conference (June 26, 2013) *available at*

data brokers could identify themselves, describe their information collection and use practices, and provide links to access tools and opt outs.

As the number of websites, apps and connected devices with which consumers interact grow exponentially, scientists, technologists and scholars correctly point out that consumers are not equipped to manage their privacy on their own.[19] For this reason, I believe that data brokers should be required to employ reasonable procedures to ensure that their clients do not use the broker's products for unlawful purposes.

Data brokers are well situated to monitor their clients' data use and sound a warning when consumers' highly sensitive information is used for unlawful purposes. Data brokers interface directly with their clients, and can assess their clients' ability to comply with existing prohibitions on discrimination. Requiring the data brokers to monitor their clients' use will create a system in which consumers are not required to bear the entire burden of managing all privacy risk associated with data brokers' profiles, and will allow those who are best situated to prevent consumer harms that would otherwise be difficult, even impossible, to detect.

The FTC also calls for legislation requiring those who provide data brokers with information to disclose to the consumer, in a clear manner, that they are sending her data on to the brokers, and to give her well-defined choices about this transfer, especially for sensitive information. This is a critical point for the consumer – the point at which the bits and bytes of each factoid about her – the flotsam and jetsam we all trail as we purchase goods online, view websites, or interact with our apps – drip into the stream that becomes the torrent that flows into her consumer profile, a dossier far removed from those initial interactions in which she shed her data.

Requiring consumer-facing data sources to provide more meaningful notice and choice to consumers is key to preserving consumer control over their privacy. In addition, such requirements tap into the competitive forces at play with respect to consumer-facing companies. We should recognize – and seek to promote – the important role that the market plays with respect to these companies. The websites, apps, and social media that deal directly with the consumer face market pressures – that other players in the ecosystem may not face – to provide their customers with data collection and use practices that protect privacy.

There is growing, and welcome, evidence that online companies are starting to compete based on their privacy promises. WhatsApp, Whisper, and Secret have grown based on their claims to provide their users with greater measures of privacy. And in this post-Snowden era,

---

http://www.ftc.gov/sites/default/files/documents/public_statements/reclaim-your-name/130626computersfreedom.pdf.

[19] *See* PCAST, BIG DATA: A TECHNOLOGICAL PERSPECTIVE, *supra* note 11, at 38 (stating that "[i]t is simply too complicated for the individual to make fine-grained choices for every new situation or app"); Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1881 (2013) (arguing that "even well-informed and rational individuals cannot appropriately self-manage their privacy" because "[i]t is virtually impossible for people to weigh the costs and benefits of revealing information or permitting its use or transfer without an understanding of the potential downstream uses," among other reasons); Mundie, *Privacy Pragmatism*, *supra* note 3 (stating that "if an individual were given the opportunity to evaluate and consent to every single act of data collection and creation that happens, he would be forced to click 'yes' or 'no' hundreds of times every day").

consumers will increasingly seek out services and tools that enhance their privacy online.[20] Indeed, Facebook, known in the past for its complex and porous privacy policies, is responding to its competition and its users by offering a "privacy checkup" to every one of its 1.28 billion users worldwide.[21] And California's Online Privacy Protection Act will soon require all online services that collect personal information from consumers residing in California to disclose more about how they respond to consumers wishes not to be tracked online,[22] which could very well lead to even more competition over privacy enhancing services and technologies.

Of course, companies that compete on privacy will need to deliver what they promise, and the FTC will watch to ensure that they do, as evidenced by the recent case of Snapchat, which promised that its app would make video and photo messages "disappear forever" after a few seconds. The FTC recently took issue with this and other promises Snapchat made, alleging the company misrepresented exactly how ephemeral the images Snapchat handled truly were.[23]

Competition and privacy concerns came together in an interesting way when the FTC considered the recently announced merger of Facebook and WhatsApp. From a competition standpoint, the FTC found instant messaging to be a vibrant marketplace in the U.S., and the merger therefore to be unproblematic. Yet there were sufficient concerns about the merger from a privacy perspective that we issued a letter to both firms underscoring that, going forward, Facebook must honor WhatsApp's existing, robust privacy policy.[24] The letter reminded Facebook that failure to honor these promises could be a violation of Section 5 of the FTC Act and, potentially, the FTC's existing consent order tackling our prior concerns about Facebook's privacy practices.

I look forward to a world where competition on privacy becomes so robust that this dimension of competition becomes baked into antitrust analysis. Although we are not there yet,[25] it is worth considering how in an appropriate case privacy might play a role in future

---

[20] Pew Research Center, Anonymity, Privacy, and Security Online 8-12 (2013), *available at* http://www.pewinternet.org/files/old-media/Files/Reports/2013/PIP_AnonymityOnline_090513.pdf (reporting results of survey that examines what steps respondents take to protect their privacy online).

[21] Vindu Goel, *Some Privacy, Please? Facebook, Under Pressure, Gets the Message*, N.Y. TIMES, at A1 (May 23, 2014), *available at* http://www.nytimes.com/2014/05/23/technology/facebook-offers-privacy-checkup-to-all-1-28-billion-users.html.

[22] CAL. BUS. & PROF. CODE § 22575, *available at* http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=BPC&sectionNum=22575; KAMALA D. HARRIS, MAKING YOUR PRIVACY PRACTICES PUBLIC 6-7 (2014), *available at* http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-issues-guide-privacy-policies-and-do-not-track.

[23] *See* Press Release, Fed. Trade Comm'n, Snapchat Settles FTC Charges That Promises of Disappearing Messages Were False (May 8, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were.

[24] Letter From Jessica L. Rich, Director of the Federal Trade Commission Bureau of Consumer Protection, to Erin Egan, Chief Privacy Officer, Facebook, and to Anne Hoge, General Counsel, WhatsApp Inc. (Apr. 10, 2014), *available at* http://www.ftc.gov/system/files/documents/public_statements/297701/140410facebookwhatappltr.pdf .

[25] The FTC has long considered mergers involving companies that compete over data, and taken appropriate remedial action where mergers of data-centric firms were likely to lead to anti-competitive outcomes. *See* In the Matter of CoreLogic, Inc., FTC File No. 131-0199; In the Matter of Fidelity National Financial, Inc./Lender Processing Services, Inc., FTC File No. 1310159.

merger analysis, both at the U.S. agencies and at DG Comp. The FTC has recognized that mergers can "adversely affect non-price attributes of competition, such as consumer privacy."[26] In the future, when examining a merger where the parties compete head-to-head for consumer eyeballs and advertising dollars based on their privacy policies, the antitrust agencies will have to investigate the same questions they ask when reviewing a merger that affects price competition: is there evidence of significant pre-merger head-to-head privacy competition between the two firms? Are they particularly close competitors in this regard? Post-merger, would this competition be replaced by competing services or successful new rivals?

In the meantime, accurate, effective, and robust information about privacy practices should generate more sunshine on how companies collect and use consumer data, spurring more competition on privacy. Consumer-facing companies providing notice and choice to their consumers thus does double duty as a strong seam in the tapestry of privacy protection.

Data Security

Some big data analytics firms believe they should be able to behave like the people profiled on the American TV show, "Hoarders:" they want to tuck away the most data possible for the longest amount of time because you never know when that can-opener-bit or this broken-chair-byte might come in handy. These big data firms argue they simply cannot delete any of this information because, by the very nature of their businesses, they themselves don't know exactly what the collected data will show or how they will eventually use it.

The unfettered collection and indefinite storage of data that is linkable to consumers[27] puts consumers at greater risk from data breaches. Bolstering data security has always been a key component of the FTC's privacy initiatives. We just filed our 53rd case involving what we alleged were unreasonable data security practices.[28] These cases have covered data security in settings ranging from pharmacy records to Internet-connected home monitoring cameras. And

---

[26] Statement of the Federal Trade Commission Concerning Google/Doubleclick; FTC File No. 071-0170.

[27] In its 2012 privacy report the Commission considers "consumer data that can be reasonably linked to a specific consumer, computer, or other device" to fall within the scope of its privacy framework. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 22, (2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [hereinafter PRIVACY REPORT]. The Commission also outlined three steps that companies may take to de-identify consumer data, so that the data is not reasonably linkable to a consumer, computer, or other device: (1) Take measures that provide a "reasonable level of justified confidence" that data cannot be linked to a consumer, computer, or other device; (2) publicly commit to maintain the data in such a fashion; and (3) contractually prohibit any recipient of the data from attempting to re-identify it. *See id.* at 21.

[28] *See* Press Release, Fed. Trade Comm'n, Snapchat Settles FTC Charges That Promises of Disappearing Messages Were False, *supra* note 23. For examples of other recent data security cases, see Press Release, Fed. Trade Comm'n, Fandango, Credit Karma Settle FTC Charges that They Deceived Consumers By Failing to Securely Transmit Sensitive Personal Information (Mar. 28, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/03/fandango-credit-karma-settle-ftc-charges-they-deceived-consumers and Press Release, Fed. Trade Comm'n, Provider of Medical Transcript Services Settles FTC Charges That It Failed to Adequately Protect Consumers' Personal Information (Jan. 31, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/01/provider-medical-transcript-services-settles-ftc-charges-it.

they provide a roadmap to what companies need to do to keep consumers' information reasonably secure.[29]

A key component of any data security plan is data minimization,[30] and that holds for big data as well as for small. In our newly released report examining the practices of data brokers, we found that, while storing data for fraud detection may make sense, the risk of hanging on to old or outdated information for marketing purposes may outweigh the benefits. For example, identity thieves and other unscrupulous actors can hack a collection of profiles that would give them a clear picture of consumers' habits over time, enabling them to predict passwords or other authentication credentials.

Like use restrictions, creative notice and choice mechanisms, and competition, data security is another thread that we must weave into our tapestry to protect consumer privacy in a world of big data.

Internet of Things

The potential benefits of the Internet of Things – self driving cars, more efficient and effective healthcare delivery – are significant. Another, less obvious benefit of the Internet of Things is its potential to spur competition and innovation as new players are brought into the Internet fold and invent better (connected) mouse traps. As a Commissioner whose mandate includes promoting competition, I see this dynamic in a positive light, and the FTC stands ready to play an appropriate role in support of the industry standardization and interoperability[31] needed to make spur entry and competition in the Internet of Things.

At the same time, I am a Commissioner whose mandate also includes privacy protection. Through this lens I see the dawn of the Internet of things threatening to unravel our tapestry approach – bringing both more challenges and a new urgency.

The FTC began two years ago to grapple with how to apply the FIPPs to a big data world in which our online and offline activities converge with the Internet of Things. Our 2012 privacy report calls for privacy by design: manufacturers of connected device should think early and often about privacy and security, and hardwire these principles into their engineering.[32] Those who design connected devices and their systems of data collection need to ensure they provide notice, choice, and transparency – crucial because consumers may not even be aware that their

---

[29] *See* Fed. Trade Comm'n v. Wyndham Worldwide Corp., Case 2:13-cv-01887-ES-JAD (Apr. 7, 2014), at 23-24 (holding that "the FTC's many public complaints and consent agreements, as well as its public statements and business guidance brochure" provide fair notice of what constitutes unfairness in the data security context) (order denying motion to dismiss).

[30] *See* Fed. Trade Comm'n, Protecting Personal Information: A Guide for Business, at 6-7 (advising companies to "[k]eep only what you need for your business); *id.* at 20-21 (advising companies to "[p]roperly dispose of what you no longer need").

[31] *See* The Internet of Things Protocol Stack – From Sensors to Business Value, Entrepreneurship Talk (Jan. 29, 2014), *available at* http://entrepreneurshiptalk.wordpress.com/2014/01/29/the-internet-of-thing-protocol-stack-from-sensors-to-business-value/.

[32] *See* PRIVACY REPORT, *supra* note 27, at 22-30.

data is being collected by devices that lack obvious interfaces. Manufacturers should deploy signals or consumer-friendly online dashboards that explain – through sounds, pictures, or graphs – the data the device collects about consumers, the uses of the data, and who else might see it. The smartphones and tablets we all carry create a ready canvas for this information.

Conclusion

I'd like to end today where I started, with another quote from *A "*Tale of Two Cities.*"* There, Dickens wrote: "A wonderful fact to reflect upon [is] that every human creature is constituted to be that profound secret and mystery to every other."[33]

For many privacy advocates, I am sure that sounds like the best of times. And for the big data analytics firms like data brokers, and their clients, the worst. In my mind, the truth is somewhere in between. We should hope for an era in which connected devices and big data analytics serve up more satisfying shopping, safer roads, cleaner air, and better health. And we should hope for an era in which, to get these benefits, we don't have to give up control over our most sensitive, private data. We reach this happy medium, not with just use restrictions, or just notice and choice mechanisms, or just competition enforcement, or just data security requirements – or even just designating the problem intractable. We reach this happy medium with a tapestry of privacy and competition protection strategies, woven one atop the other in strong yet flexible bonds.

[33] DICKENS, A TALE OF TWO CITIES, *supra* note 1, Book I, Ch. III.