CENTER FOR DEMOCRACY & TECHNOLOGY

October 27, 2017

Federal Trade Commission
Office of the Secretary
Constitution Center
400 7th Street SW, 5th Floor
Suite 5610 (Annex A)
Washington, DC 20024

Re: Informational Injury Workshop P175413

The Center for Democracy & Technology (CDT) is pleased to comment on the Federal Trade Commission's (FTC or Commission) examination of consumer injury in the context of privacy and data security. CDT is a nonprofit technology advocacy organization dedicated to promoting public policies that preserve privacy, promote innovation, and enhance individual liberties in the digital age. Our work explores the changing role of technology and data in our daily lives, investigating its impact on individuals and communities as well as the potential for data to invade privacy and cause harm.

Privacy violations are by their nature contextual, making them difficult for individuals to evaluate and regulators to quantify. Two important elements should be included in the Commission's consideration of information injury: first, user control, or lack thereof, should be an important component of the Commission's analysis of unfair acts or practices. Second, while expanded individual rights to information could serve to counterbalance the risk of privacy violations, information asymmetries limit an individual's ability to make informed decisions about privacy and security.

What are the qualitatively different types of injuries from privacy and data security incidents? What are some real life examples of these types of informational injury to consumers and to businesses?

Acting Chairman Ohlhausen has acknowledged the harms that may emerge from ubiquitous data collection and the misuse of big data technologies.[1] Privacy violations are highly contextual and can occur when information is not just used and shared, but also collected in the first instance. A survey of actions brought by the FTC and private litigants revealed that common legal claims emphasize the surreptitious collection of information, the unauthorized disclosure of personal data, unlawful retention of that information, and rampant data security failures.[2] Further, over-collection of data implicates both surveillance and other chilling effects[3] and raises documented risks of data breaches,[4] internal misuse,[5] and unwanted secondary uses of information.[6] Individuals also face the risk of inaccurate, biased, or incomplete data about themselves or their circumstances, which lead to questionable determinations that reinforce existing societal biases or eliminate accountability and insight into prejudiced decisionmaking.[7] While it is frequently argued that companies have an incentive to ensure the accuracy of their information,[8] this assumption requires scrutiny,[9] particularly as the data ecosystem grows more

[1] Maureen K. Ohlhausen, Acting Chairman, Fed. Trade Comm'n, Opening Keynote at ABA 2017 Consumer Protection Conference Atlanta (Feb. 2, 2017) (transcript available at https://www.ftc.gov/system/files/documents/public_statements/1069803/mko_aba_consumer_protection_conference.pdf).

[2] Joel R. Reidenberg et al., *Privacy Harms and the Effectiveness of the Notice and Choice Framework*, 11 I/S:J.L. & POL'Y FOR INFO. SOC'Y 485, 512 (2015). *See also* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 144 COLUM. L. REV. 583 (2014).

[3] Justin Brookman & G.S. Hans, *Why Collection Matters: Surveillance as a De Facto Privacy Harm* 1-2 (2013), *available at* https://fpf.org/wp-content/uploads/Brookman-Why-Collection-Matters.pdf.

[4] Stacy Cowley & Tara Siegel Bernard, *As Equifax Amassed Ever More Data, Safety Was a Sales Pitch*, N.Y. TIMES (Sept. 23, 2017), https://www.nytimes.com/2017/09/23/business/equifax-data-breach.html ("But this strategy means that Equifax is entrenched in consumers' financial lives whether they like it or not — or even know it. Equifax's approach amplified the consequences of the breach, reported this month, that exposed the personal information for up to 143 million people.").

[5] *See, e.g.*, Johana Bhuiyan & Charlie Warzel, *"God View": Uber Investigates Its Top New York Executive For Privacy Violations*, BUZZFEED (Nov. 18, 2014), https://www.buzzfeed.com/johanabhuiyan/uber-is-investigating-its-top-new-york-executive-for-privacy. More recently, the FTC brought a complaint against Uber Technologies alleging the company was deceptive in how it monitored employee access to information. FTC Complaint In the Matter of Uber Technologies, Inc., No. 1523054 (Aug. 2017), https://www.ftc.gov/system/files/documents/cases/1523054_uber_technologies_complaint.pdf.

[6] In the Matter of AnchorFree, Inc. Hotspot Shield VPN (Aug. 7, 2017) (CDT Complaint, Request for Investigation, Injunction, and Other Relief), https://cdt.org/files/2017/08/FTC-CDT-VPN-complaint-8-7-17.pdf (arguing that undisclosed and unclear data sharing and traffic redirection with advertisers and other third parties when using a VPN is an unfair business practice).

[7] ALETHEA LANGE, DIGITAL DECISIONS: POLICY TOOLS IN AUTOMATED DECISION-MAKING, CTR. FOR DEMOCRACY & TECH. (Jan. 14, 2016), https://cdt.org/files/2016/01/2016-01-14-Digital-Decisions_Policy-Tools-in-Auto2.pdf.

[8] Separate Statement of Commissioner Maureen K. Ohlhausen, Big Data A Tool for Inclusion or Exclusion? A-1 (Jan. 2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-

opaque, centralized and reliant on common data sources and datasets to inform predictive models. This concern is especially salient when common, public sources of information are used for purposes of training machine learning models.[10]

Attempts have been made to identify and categorize these types of privacy violations in ways that lawmakers and policymakers can understand. In its guide to privacy engineering and risk management for federal systems, the National Institute for Standards & Technology (NIST) explains that the range of potential risks that arise from the processing of personal information includes not just economic loss but also diminished capacity for autonomy and self-determination, discrimination (legal or otherwise), and a generalized loss of trust.[11] NIST's framework is itself an adaptation of Professor Daniel Solove's detailed taxonomy of privacy that looks at the problematic activities that emerge from information collection, processing, and dissemination.[12] Both Professor Solove and NIST acknowledge that their categorizations are non-exhaustive, but they also recognize that having a broad understanding of privacy risk is essential in order to address user concerns.

These injuries ultimately are the byproduct of and flow from questions around who should control information online. This principle was placed front and center, prior to any other consumer right, in the 2012 Obama White House Privacy Bill of Rights, which declared that individuals "have a right to exercise control over what personal data companies collect from them and how they use it."[13] Americans also want more control. A 2016 survey from Pew

---

issues/160106big-data-rpt.pdf ("Our competition expertise tells us that if one company draws incorrect conclusions and misses opportunities, competitors with better analysis will strive to fill the gap.").

[9] For example, the FTC has regularly found significant incidences of error in consumer credit reporting. *See* FED. TRADE COMM'N, REPORT TO CONGRESS UNDER SECTION 319 OF THE FAIR AND ACCURATE CREDIT TRANSACTIONS ACT OF 2003 (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/section-319-fair-accurate-credit-transactions-act-2003-sixth-interim-final-report-federal-trade/150121factareport.pdf.

[10] For example, a set of 1.6 million publicly released emails from Enron in 2003 have become a shared data source. April Glaser, *Who Trained Your A.I.?*, SLATE (Oct. 24, 2017), http://www.slate.com/articles/technology/technology/2017/10/what_happens_when_the_data_used_to_train_a_i_is_biased_and_old.html (citing Amanda Levindowski, *How Copyright Law Can Fix Artificial Intelligence's Implicit Bias Problem* (July 24, 2017), *available at:* https://ssrn.com/abstract=3024938).

[11] Sean Brooks et al., NISTIR 8062 An Introduction to Privacy Engineering and Risk Management in Federal Systems 10 (Jan. 2017), http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf.

[12] Daniel Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006). In addition to violations of information privacy, Professor Solove also describes "invasions" that directly impinge on individuals without necessarily involving access to information about them.

[13] CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY, THE EXECUTIVE OFFICE OF THE PRESIDENT 2012). The Consumer Privacy Bill of Rights was

Research found that 74% of those surveyed believe it is "very important" to be in control over *who gets acces*s to their information and 65% want control over *what information is collected* about them.[14] Unfortunately, policy discussions around big data analytics, machine learning applications, and innovations in the Internet of Things often discount the role of user control, instead arguing that new technologies should address privacy concerns through corporate accountability measures and some undefined limitations on how companies use data.[15]

Individuals thus rightly perceive that they lack control over how information about them is collected, shared, and used. Another Pew Research survey worryingly found that 91% of those surveyed believe that they have lost control over how their information is used by companies; similarly large percentages of American express concerns about the accuracy of this information.[16] This leads to the pervasive fears, discomforts, and other chilling effects that are emblematic of what Professor Ryan Calo has described as subjective privacy harms.[17] These perceptions are then borne out by vivid examples of individuals, even the most privacy conscious, being subjected to an opaque digital ecosystem that offers limited options for controlling how information is collected, used, and shared.

When individuals wish to protect their privacy, the challenge confronting them can be extreme. Take, for example, research by Janet Vertesi and Kashmir Hill into the demand for data about pregnant women and other would-be mothers. Vertesi went to great lengths to conceal her pregnancy from marketers and companies who prize the commercial value of pregnant women.[18] She not only had to police the activities of friends and family on social media, but she

---

modeled after Fair Information Practice Principles-based international frameworks, including the Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the Asia-Pacific Economic Cooperation (APEC) Privacy Framework.

[14] Lee Rainie, Pew Research Center, *The state of privacy in post-Snowden America* (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/.

[15] Ctr. for Democracy & Tech., Comments to the FTC after November 2013 Workshop on the "Internet of Things" (Jan. 10, 2014), *available at* https://cdt.org/files/pdfs/iot-comments-cdt-2014.pdf [hereinafter CDT IoT Comments].

[16] Mary Madden, Pew Research Center, *Public Perceptions of Privacy and Security in the Post-Snowden Era* (Nov. 12, 2014), http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/.

[17] M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1143 (2011).

[18] Janet Vertesi, Opinion, *My Experiment Opting Out of Big Data Made Me Look Like a Criminal*, TIME (Apr. 30, 2014), http://time.com/83200/privacy-internet-big-data-opt-out/. Pregnancies are especially appealing to marketers because they are significant life events impacting an "emotionally charged group" likely to shift spending habits and brand loyalty. *See* CHARLES DUHIGG, THE POWER OF HABIT: WHY WE DO WHAT WE DO IN LIFE AND BUSINESS (2012); Sharon Cole, *Market Focus: Expectant Mother*s, TARGETMARKETING (June 1, 2004),

and her husband had to make elaborate uses of the Tor browser, gift cards, and false addresses to obscure her digital footprint. These efforts to maintain control over what Vertesi considered to be intensely private information created a digital profile that made her, in her own words, "look like a criminal." More recently, Hill took the opposite approach, collaborating with the Electronic Frontier Foundation to monitor and study information flows and data leakage about her pregnancy via nineteen different fertility and pregnancy tracking apps.[19] Their research found a number of privacy and security issues, including the expected array of third party tracking technologies as well as data leakage and deletion issues.[20]

The precise information injury to expectant mothers may not be clear (though it was very obvious in at least one famous case)[21], but they demonstrate the specter of exposure and other reputational violations that can occur. One of the core values of information privacy is its utility in creating space for nurturing political thought and preventing the unwarranted disclosure and discriminatory use of intimate knowledge,[22] but opaque information flows can upset this expectation. In recent months, for example, reports emerged about how social network features that recommend new potential contacts could effectively expose sex workers and other privacy-conscious individuals.[23] These features generally rely on mutual connections and shared networks to suggest additional contacts,[24] but there are often other proprietary elements to how these mechanisms work and limited ability for user's to opt-out of their use.[25] While this is a common industry practice, the result of this opacity is an experience that can harm individuals at worst and in some cases, violate their expectations.

---

http://www.targetmarketingmag.com/article/market-focus-expectant-mothers-28713/all/. Vertesi also notes that value of a pregnant woman's marketing data is worth approximately $1.50 compared to just 10 cents for the average person.

[19] Kashmir Hill, *What Happens When You Tell the Internet You're Pregnant*, GIZMODO (July 27, 2017), https://jezebel.com/what-happens-when-you-tell-the-internet-youre-pregnant-1794398989.

[20] COOPER QUINTIN, THE PREGNANCY PANOPTICON, ELECTRONIC FRONTIER FOUNDATION (July 2017), https://www.eff.org/files/2017/07/27/the_pregnancy_panopticon.pdf.

[21] Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

[22] Scott Skinner-Thompson, *Outing Privacy*, 110 NW. U. L. REV. 159, 162 (2015).

[23] Kashmir Hill, *How Facebook Outs Sex Workers*, GIZMODO (Oct. 11, 2017), https://gizmodo.com/how-facebook-outs-sex-workers-1818861596.

[24] Finding Friends and People You May Know, Facebook, https://www.facebook.com/help/www/336320879782850 (last visited Oct. 20, 2017).

[25] Hill, *supra* note 23.

As the example above illustrates, individuals have limited insight into the complexity of information flows in digital systems and how their personal information may ultimately be used. Individuals also lack user controls that are responsive to the creative ways entities monetize user data. Recently, a team of researchers at the University of Washington explored how targeting online behavioral advertisements can be used to track the locations and activities of targeted individuals, without their knowledge or consent, as they move from home to work and beyond.[26] A motivated attacker could use ad purchase to count the number of users at a household level of potentially sensitive apps like Grindr, which is used by gay, bisexual, or queer men, or Quran Reciters and know exactly when and where the apps are being used.[27]

What frameworks might we use to assess these different injuries? How do we quantify injuries? How might frameworks treat past, current, and potential future outcomes in quantifying injury? How might frameworks differ for different types of injury?

The context in which information is collected and used has become an important part of understanding individuals' privacy expectations. While context has been warmly embraced in principle, in practice, the notion that context should be respected have frequently been framed by industry as a proxy for simply providing "notice."[28] As Professor Helen Nissenbaum explains, context can be shaped by business practices, industry sectors, and technologies, but her initial theory of contextual integrity emphasized social norms around information sharing that promote ethics and other important societal values.[29] Expectations may evolve over time, but privacy violations must not be based upon industry's exclusive determinations about when data usage is in context or not. The novelty of a product or service is not a salve to data practices that run contrary to an individual's reasonable expectations about how their personal information is protected or shared.[30]

---

[26] Paul Vines, Franziska Roesner, and Tadayoshi Kohno, Exploring ADINT: Using Ad Targeting for Surveillance on a Budget — or — How Alice Can Buy Ads to Track Bob (2017), *available at* https://adint.cs.washington.edu.

[27] Andy Greenberg, *It Takes Just $1,000 to Track Someone's Location With Mobile Ads*, WIRED (Oct. 18, 2017), https://www.wired.com/story/track-location-with-mobile-ads-1000-dollars-study/.

[28] *See, e.g.*, PRIVACY PRINCIPLES FOR VEHICLE TECHNOLOGIES AND SERVICES 9 (Nov. 2014), https://autoalliance.org/wp-content/uploads/2017/01/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services.pdf ("When Participating Members present clear, meaningful notices about how Covered Information will be used and shared, that use and sharing is consistent with the context of collection.").

[29] Helen Nissenbaum, *"Respect for Context": Fulfilling the Promise of the White House Report*, in PRIVACY IN THE MODERN AGE: THE SEARCH FOR SOLUTIONS, eds. M. Rotenberg, J. Horwitz, J. Scott, EPIC 152-164 (2015).

[30] *See* CDT IoT Comments, *supra* note 15.

Respecting context is not, however, a substitute for careful deployment of the Fair Information Practice Principles (FIPPs).[31] CDT has explained how the FIPPs remain relevant in online privacy,[32] big data,[33] and the Internet of Things,[34] and the Commission must continue to focus on promoting and enforcing a comprehensive set of the FIPPs. Key FIPPs principles relevant to information injury include: requiring transparency and notice of data collection practices, providing consumers with meaningful choice regarding the use and disclosure of that information, allowing consumers reasonable access to the personal information they have provided, providing remedies for misuse or unauthorized access, and setting standards to limit data collection and ensure data security.

To further these principles in the context of informational injury, we believe the Commission must aggressively exercise its unfairness authority under Section 5 of the FTC Act. In contrast to the Commission's deception authority, unfairness may be better equipped to address structurally problematic privacy practices. In a 2000 address on "unfairness", former FTC Commissioner Thomas Leary framed unfairness authority as a tool best deployed in circumstances where unfair conduct is done by third parties with which consumers have no relationship, or where practices prey on vulnerable consumers, involve coercive conduct, or create significant information deficits.[35] Leary thought this captured the worst actors in the early online ecosystem, but it remains an apt description of an environment that continues to challenge – and violate – individual privacy on a regular basis. Unfairness has broader reach than deception as an enforcement mechanism to address problematic privacy practices.[36] For a potential privacy violation to be deemed unfair, the act or practice must cause or be likely to cause (1) substantial injury to consumers (2) that cannot be reasonably avoidable (3) and are

[31] *See, e.g.,* Nat'l Inst. of Standards & Tech. (NIST), National Strategy for Trusted Identities in Cyberspace, app. A (April 2011), *available at* https://cryptome.org/2014/11/nstic-fipps.pdf.

[32] Ctr. for Democracy & Tech., Refocusing the FTC's Role in Privacy Protection: Comments to the FTC Consumer Privacy Roundtable (2009), *available at* https://www.ftc.gov/sites/default/files/documents/public_comments/privacy-roundtables-comment-project-no.p095416-544506-00026/544506-00026.pdf.

[33] Ctr. for Democracy & Tech., Comments to the Office of Science and Technology re: Big Data Study (Mar. 31, 2014), https://www.cdt.org/files/pdfs/Big-Data.pdf.

[34] CDT IoT Comments, *supra* note 15.

[35] Thomas B. Leary, Unfairness and the Internet (Apr. 13, 2000), https://www.ftc.gov/public-statements/2000/04/unfairness-and-internet.

[36] On the other hand, use of the unfairness authority demands a more detailed fact-finding exercise on the part of the Commission.

not offset by benefits to consumers. Importantly, larger public policy considerations, including state laws and self-regulatory guidance, must also play a role in this analysis.

One way to mitigate privacy violations and resulting injuries to individuals is through the enactment and enforcement of meaningful user controls. For example, the Commission should consider, in its unfairness analysis, the relationship between privacy violations being "reasonably avoidable" and the FIPPs associated with data access, integrity, and user control. The Commission assumes that individuals are generally in a position to "survey the available alternatives, choose those that are most desirable, and avoid those that are inadequate or unsatisfactory."[37] Some have suggested the lack of control does not meet this test because individuals can avoid any potential harm by merely not using a service.[38] But this assumption is increasingly ill-suited to today's digital environment, especially where data-driven services in consumer products ranging from toys to televisions are provided to consumers not as an add-on service but as an integral function of the device.[39] The Commission has begun to face this challenge in its recent enforcement action against Vizio, alleging that explicit consent is needed for a smart television can capture robust television viewing behavior habits.[40] While the action largely focused on the sensitivity of the information involved and Vizio's failure to provide prominent and easily understandable disclosures, the failure to provide better user functionality and control over their information is a salient fact of the case, as well. In light of the examples above, it's clear that individuals can no longer reasonably avoid many day-to-day privacy violations.

However, user controls must be more than rote "opt-in" and "opt-out" mechanisms. Privacy violations occur when companies forget that individuals have an ongoing interest in their information. Omer Tene and Jules Polonetsky lament that the right to access information remains "woefully underutilized."[41] They argue that companies have developed access

[37] Letter from FTC Comm'rs to Wendell H. Ford & John C. Danforth, Senators (Dec. 17, 1980), reprinted in In re Int'l Harvester Co., 104 F.T.C. 949 app. at 1070–76 (1984) (FTC Policy Statement on Unfairness), *available at* https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.

[38] Justin Brookman, *Protecting Privacy in an Era of Weakening Regulation*, 9 HARV. L. & POL'Y REV. 355, 359 (2015).

[39] Michael Vax, *Commerce trends: Moving from goods to services* (Apr. 10, 2015), http://www.the-future-of-commerce.com/2015/04/10/commerce-trends-moving-from-things-you-sell-to-services-you-provide/.

[40] FTC, et al. v. Vizio, Inc., Case No. 2:17-cv-00758 (Feb. 6, 2017)(U.S. Dist. Court, Dist. of NJ), https://www.ftc.gov/system/files/documents/cases/170206_vizio_stipulated_proposed_order.pdf.

[41] Omer Tene and Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239, 263 (2013).

mechanisms that are neither convenient nor useful. "Organizations often fail to provide details about sources, uses, and recipients of the information they collect, and seek to rely on a panoply of legal exemptions to mask portions of the data that they do disclose," they explain. When the Commission began to develop its expertise in online privacy in 2000, it noted that user access to information presented unique implementation challenges for companies including the scope of information made available, the costs and benefits of providing access, and adequate authentication measures.[42]

CDT has previously argued that more sensors and more connectivity provide an opportunity to create stronger and more usable control mechanisms.[43] At the same time, individual rights of access, restriction, and portability in the forthcoming EU General Data Protection Regulation (GDPR) also provide a further catalyst for advances in user controls. While Americans may not have legally codified privacy rights like EU citizens, market pressures may pressure the global adoption of GDPR-esque user controls. To the extent that commercial entities offer innovative processes and tools within the European Union, companies should grant Americans the same ability to take advantage of these mechanisms.

For example, data access rights under European Union law are already robust and have been used to pressure companies into providing portals and other mechanisms to "download" consumer data.[44] Recently, a data access request to the dating app Tinder resulted in one European user receiving approximately 800 pages of information about her online dating activities.[45] This information gave the user additional transparency into her sexual preferences and treatment of potential suitors; her request also provided insight into the wealth of information she was implicitly disclosing to the app about her romantic desires and inclinations.[46]

---

[42] FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE -- A REPORT TO CONGRESS 17 (May 2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.

[43] CDT IoT Comments, *supra* note 15, at 9.

[44] Olivia Solon, *How much data did Facebook have on one man? 1,200 pages of data in 57 categories*, WIRED (Dec. 2012), http://www.wired.co.uk/article/privacy-versus-facebook.

[45] Judith Duportail, *I asked Tinder for my data. It sent me 800 pages of my deepest, darkest secrets*, GUARDIAN (Sept. 26, 2017), https://www.theguardian.com/technology/2017/sep/26/tinder-personal-data-dating-app-messages-hacked-sold.

[46] The reporter laments that "Tinder is how I meet people, so this is my reality. It is a reality that is constantly being shaped by others – but good luck trying to find out how." *Id.*

The pages of raw data may not be extremely useful, as Tene and Polonetsky suggest, but the GDPR's new "right to data portability" may spur new approaches in this area. Article 20 will require that companies provide EU data subjects with personal data "in a structured, commonly used and machine-readable format" and have the ability to transmit that information elsewhere "without hindrance." The contours of this portability right are unclear,[47] but CDT believes data portability has tremendous potential to empower users and increase their control in the data ecosystem.[48] The Commission has already noted the importance of data portability in the Internet of Things, and it should study the policy and technical challenges of data portability and to evaluate new practices through the Office of Technology Research and Investigation.[49] When companies do not offer meaningful controls, including access to information and the ability to port data and permanently close accounts, they make privacy harms unavoidable and unfair.

How do consumers perceive and evaluate the benefits, costs, and risks of sharing information in light of potential injuries? What obstacles do they face in conducting such an evaluation?

Industry has argued that privacy debates disproportionately weigh the interest of privacy-sensitive individuals against the interests of other consumers and industry innovation.[50] This stems from an intuitive but flawed division of individuals into three main buckets: privacy fundamentalists, privacy pragmatists, and the privacy unconcerned.[51] According to this framework, pragmatists weigh the costs and benefits of services and make choices that are consistent with their privacy preferences -- which are generally assumed to be less rigid than

[47] Article 29 Data Protection Working Party, Guidelines on the Right to Data Portability WP 242 (Dec. 13, 2016), http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf.

[48] Ctr. for Democracy & Tech., Comments to the Office of Science of Technology Policy re: Data Portability 7-8 (Nov. 23, 2016), https://cdt.org/files/2016/11/OSTP-Data-Portability-Comments-11-23-16.pdf. Portability raises its own challenges, but promises fruitful conversations separate from traditional privacy debates. *See Washington vs. Big Tech: Should you "own" all your social network data? An AEIdeas online symposium*, AMERICAN ENTERPRISE INSTITUTE (Oct. 10, 2017), www.aei.org/publication/washington-vs-big-tech-should-you-own-all-your-social-network-data-an-aeideas-online-symposium/; Will Rinehart, *The Social Graph Portability Act Doesn't Take Tech Seriously, and That's Worrying*, TECH POLICY CORNER (Oct. 13, 2017), https://techpolicycorner.org/the-social-graph-portability-act-doesnt-take-tech-seriously-and-that-s-worrying-63c7259a6fec.

[49] *Id*. at 7-8.

[50] Alex McQuinn, Info. Tech. & Innovation Foundation, *The Economics of "Opt-Out" Versus "Opt-In" Privacy Rules* (Oct. 6, 2017), https://itif.org/publications/2017/10/06/economics-opt-out-versus-opt-in-privacy-rules; *see also* Remarks of Commissioner Maureen K. Ohlhausen at the Digital Advertising Alliance Summit 3 (June 5, 2013), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-commissioner-maureen-k.ohlhausen/130605daasummit.pdf.

[51] LOUIS HARRIS & ALAN WESTIN, EQUIFAX/HARRIS CONSUMER PRIVACY SURVEY 13 (1996).

privacy fundamentalists. This has been the Commission's operating assumption about how the market for privacy works.

This is inaccurate. Surveys have repeatedly shown the individuals face pervasive information asymmetries online.[52] According to research by Professors Jennifer Urban and Chris Hoofnagle, the knowledge deficits impacting the so-called privacy pragmatists preclude them from taking truly pragmatic action in the marketplace.[53] The examples detailed above also demonstrate how the opacity in online data flows further hampers individual's ability to meaningfully evaluate privacy risks and potential benefits. It is difficult for consumers to weigh the future risk to their privacy against immediate conveniences, and the information needed to make this determination can be considerable. For example, EFF's research into the many privacy and security issues posed by fertility apps concludes that "women should carefully consider the privacy and security tradeoffs before deciding to use any of these applications."[54] But there is no reasonable way for an expectant mother to, first, have access to the information that could violate their privacy and, second, understand how those risks could emerge over time. Hill noted in her reporting that while these apps were beneficial to her, she would "spare any future fetuses the pregnancy panopticon."[55] This was a determination that required at least nine months, consider technical research, and as Vertesi put it when she discussed her own pregnancy, any single slip up would let "the cat out of the bag."[56]

Knowledge gaps exist for privacy fundamentalists, as well. For example, privacy-conscious consumers interested in protecting their network traffic by using a virtual private network (VPN) face an ecosystem of different providers, business models, and options that can pose an "impossible task" for individuals.[57] As CDT's recent complaint against AnchorFree HotSpot

[52] *See* Aaron Smith, Pew Research Center, *Half of online Americans don't know what a privacy policy is* (Dec. 4, 2014), http://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is/; Acquisti, Alessandro, Curtis Taylor & Liad Wagman, *The Economics of Privacy*, JOURNAL OF ECONOMIC LITERATURE 54, no. 2 (2016): 442-492.

[53] Chris Jay Hoofnagle & Jennifer M. Urban, *Alan Westin's Privacy Homo Economicus*, 49 WAKE FOREST L. REV. 261 (2014).

[54] Quintin, *supra* note 20, at 3.

[55] Hill, *supra* note 19.

[56] Janet Vertesi (@cyberlyra), Twitter (Apr. 26, 2014, 12:11 AM), https://twitter.com/cyberlyra/status/459907600298299392?ref_src=twsrc%5Etfw&ref_url=http%3A%2F%2Fmashable.com%2F2014%2F04%2F26%2Fbig-data-pregnancy%2F.

[57] Yael Grauer, *The impossible task of creating a "Best VPNs" list today*, ARSTECHNICA (June 1, 2016), https://arstechnica.com/information-technology/2016/06/aiming-for-anonymity-ars-assesses-the-state-of-vpns-in-2016/; *see also* Brian Krebs, *Post-FCC Privacy Rules, Should You VPN?*, KREBSONSECURITY (Mar. 30, 2017),

Shield VPN details, users are tasked with scrutinizing marketing statements, privacy policies, and terms of service that send conflicting and vague messages,[58] and even if a given VPN provider makes clear and express disclosures, it can be difficult for individuals to know exactly what type of protections they are getting from their chosen VPN. This is not merely a question of deceptive business practices, but for privacy-conscious consumers who resolutely want control over their information, it creates an information asymmetry that violates user self-determination.

If the Commission's position is that consumers should have options that comport with their privacy preferences,[59] it must first acknowledge that individual privacy preferences are shaped by numerous factors including not just knowledge about privacy protections and business practices generally but also exposure to identity theft, stalking, or an error-ridden credit report or consumer profile; race; gender; socioeconomic class; and attitudes toward government and law enforcement.[60] Through its enforcement, educational, and investigatory efforts, the FTC can work to address this gap.

Thank you for the opportunity to comment. Please contact me at 202.407.8831 if you have any questions.

Sincerely,

Michelle De Mooy
Director, Privacy and Data Project

Joseph Jerome
Policy Counsel, Privacy and Data Project

Natasha Duarte
Policy Analyst, Privacy and Data Project

Kayvan Farchadi
Intern, Privacy and Data Project

https://krebsonsecurity.com/2017/03/post-fcc-privacy-rules-should-you-vpn/; Brian X. Chen, *For Internet Privacy, VPNs Are an Imperfect Shield*, N.Y. TIMES (Apr. 5, 2017), https://www.nytimes.com/2017/04/05/technology/personaltech/vpn-internet-security.html.

[58] In the Matter of AnchorFree, Inc. Hotspot Shield VPN (Aug. 7, 2017) (CDT Complaint, Request for Investigation, Injunction, and Other Relief), https://cdt.org/files/2017/08/FTC-CDT-VPN-complaint-8-7-17.pdf.

[59] Ohlhausen, *supra* note 50, at 4.

[60] Jennifer M. Urban & Chris Jay Hoofnagle, *The Privacy Pragmatic as Privacy Vulnerable* 4 (2014), https://cups.cs.cmu.edu/soups/2014/workshops/privacy/s1p2.pdf.