

December 20, 2018

Constitution Center  
Federal Trade Commission  
400 7<sup>th</sup> Street, SW  
Washington, DC 20024

Dear Federal Trade Commission,

On behalf of Public Knowledge, a public interest advocacy organization dedicated to promoting freedom of expression, an open internet, and access to affordable communications tools and creative works, we were grateful for the opportunity to testify at the Federal Trade Commission’s Hearings on Competition and Consumer Protection in 21st Century: Big Data, Privacy, and Competition, and we welcome the opportunity to submit these comments, in response to Docket ID: FTC-2018-0100, reflecting on the hearings.

It is no longer possible to participate in society without providing data to third parties that may, in and of themselves be personal, or that, when combined with other data and analyzed, may reveal intimate information. The consequences of this data acquisition, analysis, use, and sharing can be profound for individuals’ lives. For example, data have been used to show certain job postings only to men<sup>1</sup> and to exclude African-Americans from seeing certain housing advertisements.<sup>2</sup> During the 2016 election, Russian agents were able to use data to target advertisements to African-Americans to urge them not to vote.<sup>3</sup> Data exploitation enables “unequal consumer treatment, financial fraud, identity theft, manipulative marketing, and discrimination.”<sup>4</sup> Against this backdrop, the FTC’s hearings on Big Data, Privacy, and Competition could not have been timelier. These comments will memorialize Public Knowledge’s testimony and primary takeaways from the hearings and address two of the specific questions posed in the FTC’s request for comments.

## **2. How have developments involving data – data resources, analytic tools, technology, and business models – changed the understanding and use of personal or commercial information or sensitive data?**

In 2002, Target wanted to identify expectant parents in their second trimester, recognizing that one of the moments when people’s buying patterns change is when they have a child. Target believed that if it captured loyal shoppers in their second trimester, it would keep them for years. It started tracking customers who had Target baby registries and discovered that around their second trimester, they began buying larger quantities of unscented lotion as well as calcium, magnesium, and zinc supplements. All told, Target identified 25 products that enabled them to assign

---

<sup>1</sup> See UPTURN, *LEVELING THE PLATFORM: REAL TRANSPARENCY FOR PAID MESSAGES ON FACEBOOK* (May 2018).

<sup>2</sup> Julia Angwin, Ariana Tobin, and Madeleine Varner, *Facebook (Still) Letting Housing Advertisers Exclude Users By Race*, PROPUBLICA, Nov. 21, 2017.

<sup>3</sup> Natasha Singer, *Just Don’t Call It Privacy*, NY TIMES, Sept. 23, 2018, <https://www.nytimes.com/2018/09/22/sunday-review/privacy-hearing-amazon-google.html>.

<sup>4</sup> *Id.*

customers a “pregnancy prediction score” – even if the customer did not have a Target registry. Target was also able to identify customers’ due dates within a narrow window so that it could send coupons timed to specific stages of pregnancy.<sup>5</sup> Data-driven advertising has only mushroomed since 2002, particularly as individuals spend more and more of our lives online.

Data-driven online advertising allows customized online experiences for individual consumers. Targeted advertising, may reduce irrelevant ads, help consumers discover new, relevant products, and/or make online shopping easier.<sup>6</sup> And, data-driven advertising may be particularly helpful for small businesses with specialized or local products that are trying to reach a very niche audience.

However, data-driven online advertising may also facilitate higher prices and reduce competition. Algorithms can monitor prices and other terms of sale,<sup>7</sup> giving companies a more detailed view of the market in nearly real-time,<sup>8</sup> allowing them to adjust to market changes more quickly and reliably,<sup>9</sup> and diminishing their need to cut prices to stay competitive.<sup>10</sup> Notably, this practice is likely not redress-able under existing antitrust law, because it does not involve an express agreement to fix prices.

Moreover, pervasive data collection, sharing, aggregation, and use allow companies to develop detailed profiles of their customers’ psychologies<sup>11</sup> and willingness to pay.<sup>12</sup> This enables “personalized pricing strategies”<sup>13</sup> with precise manipulations of consumer choices.<sup>14</sup> These insights into, and power over, customer behavior ultimately may help firms maximize profit to the net detriment of their customers.<sup>15</sup> This sort of data-crunching and personalized advertising on a person-by-person basis used to be unimaginable, but algorithms, machine learning, and big data make this type of personalized advertising not only possible, but scalable.

---

<sup>5</sup> Charles Duhigg, *How Companies Learn Your Secrets*, NY TIMES, Feb. 16, 2012, <https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html>.

<sup>6</sup> David Kirkpatrick, *Study: 71% of consumers prefer personalized ads*, MARKETING DIVE, May 9, 2016, <https://www.marketingdive.com/news/study-71-of-consumers-prefer-personalized-ads/418831/>.

<sup>7</sup> *Id.*

<sup>8</sup> Maurice E. Stucke & Ariel Ezrachi, *How Pricing Bots Could Form Cartels and Make Things More Expensive*, HARV. BUS. REV., Oct. 27, 2016, <https://hbr.org/2016/10/how-pricing-bots-could-form-cartels-and-make-things-more-expensive>.

<sup>9</sup> Michal S. Gal, *Algorithmic-Facilitated Coordination: Market and Legal Solutions*, CPI ANTITRUST CHRONICLE, May 2017, <https://www.competitionpolicyinternational.com/wp-content/uploads/2017/05/CPI-Gal.pdf>.

<sup>10</sup> A. Erachi & M.E. Stucke, Note, *Algorithmic Collusion: Problems and Counter-Measures*, 25 OECD ROUNDTABLE ON ALGORITHMS & COLLUSION, 1, 6 (2017).

<sup>11</sup> Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995 (2014).

<sup>12</sup> A. Erachi & M.E. Stucke, Note, *Algorithmic Collusion: Problems and Counter-Measures*, 25 OECD ROUNDTABLE ON ALGORITHMS & COLLUSION, 1, 12 (2017).

<sup>13</sup> *Id.*

<sup>14</sup> Michal Gal & Niva Elkin-Koren, *Algorithmic Consumers*, 30 HARV. J. OF L. & TECH. 309, 324 (2017).

<sup>15</sup> Ramsi A. Woodcock, *The Power of the Bargaining Robot*, CPI ANTITRUST CHRONICLE, May 2017, <https://www.competitionpolicyinternational.com/wp-content/uploads/2017/05/CPI-Woodcock.pdf>; *see also* Michal S. Gal, *Algorithmic-Facilitated Coordination: Market and Legal Solutions*, CPI ANTITRUST CHRONICLE, May 2017, <https://www.competitionpolicyinternational.com/wp-content/uploads/2017/05/CPI-Gal.pdf>.

The available data bear out that this sort of “personalized pricing” is often not welfare enhancing for consumers. For example, “the lowest prices are more likely to be found in organic search results rather than in sponsored search results,”<sup>16</sup> which are more likely to be “personalized.” Similarly, Professor Ramsi Woodcock testified at the FTC’s hearings that targeted advertising “allows firms to increase the willingness of consumers to pay for products that, absent the advertising, they would not, in fact, prefer.”<sup>17</sup> Moreover, Professor Ramsi explained that data “allows firms to figure out how much they can raise prices without alienating their consumers. So it allows for them to extract more value from consumers for any given level of competition in the market.”<sup>18</sup> In short, there are “distributional” effects of big data and personalized pricing, and those effects disproportionately benefit firms over individual consumers.<sup>19</sup>

Importantly, this type of sophisticated analytics renders the so-called sensitive/non-sensitive distinction illogical for today’s world. So-called non-sensitive information can be aggregated to reveal sensitive information, and, in fact, some non-sensitive information, in isolation, may reveal sensitive information. For example, while one’s health status is frequently considered sensitive, one’s shopping history is not. Therefore, the personal information Target used to determine its shoppers’ pregnancy status would not be classified as sensitive – even though the information was used as an effective proxy for health status. In addition, sometimes, a single, purportedly non-sensitive data point in isolation, such as the fact that one is shopping at TLC Direct<sup>20</sup> and Headcovers Unlimited,<sup>21</sup> two websites that specialize in hats for chemotherapy patients, may be sufficient to reveal sensitive information. In fact, when companies advocate for a sensitive/non-sensitive distinction, they may be counting on their “ability to infer latent data from surface information,”<sup>22</sup> recognizing that “people cannot know what they are really revealing when they decide to hand over surface information”<sup>23</sup> and that companies can easily monetize the revealed latent information. For this reason, among others,<sup>24</sup> any line drawing around the sensitivity of information is inherently arbitrary. Thus, any federal privacy regime must provide robust protections for all personal information – that is, any information that is reasonably

---

<sup>16</sup> Alessandro Acquisti, Professor of Information Technology and Public Policy, Heinz College, Carnegie Mellon University, *The Economics of Big Data and Personal Information*, Testimony before the FTC Hearings on Big Data, Privacy, and Competition (Nov. 6, 2018).

<sup>17</sup> Ramsi Woodcock, Assistant Professor of Law, University of Kentucky College of Law, *Perspectives on Data Policy*, Testimony before the FTC Hearings on Big Data, Privacy, and Competition (Nov. 8, 2018).

<sup>18</sup> *Id.*

<sup>19</sup> *Id.*

<sup>20</sup> TLC DIRECT, <https://www.tlcdirect.org> (last visited Nov. 2, 2018).

<sup>21</sup> HEADCOVERS UNLIMITED, <https://www.headcovers.com> (last visited Nov. 2, 2018).

<sup>22</sup> Dennis Hirsch, Professor of Law and Director of the Program on Data and Governance, The Ohio State University Moritz College of Law, *Corporate Data Ethics: Risk Management for the Big Data Economy*, Testimony before the FTC Hearings on Big Data, Privacy, and Competition (Nov. 6, 2018).

<sup>23</sup> *Id.*

<sup>24</sup> So-called non-sensitive information can be used for purposes that are quite sensitive. For example, if Cambridge Analytica (and, for that matter, the Obama campaign, Tim Murphy, *Inside the Obama Campaign’s Hard Drive*, MOTHER JONES, Sept./Oct. 2012, <https://www.motherjones.com/politics/2012/10/harper-reed-obama-campaign-microtargeting/>) is to be believed, so-called non-sensitive information like social media likes can be used for highly sensitive activities such as influencing individuals in the voting booth. In addition, sensitivity is highly subjective. Different individuals are likely to perceive different data points’ sensitivity levels differently.

linkable, directly or indirectly, to a specific consumer, household, or device<sup>25</sup> – and not merely for so-called sensitive information.

Data-driven online advertising also may foreclose opportunities for consumers – when data are used to determine what ads are “relevant” to a particular consumer, that consumer is most often unaware of the options he or she never sees. That may be more or less pernicious depending on the subject of the advertisement. For example, if the ads are for housing or job opportunities, the data-driven omission may be particularly problematic. This problem is not conjecture: employers have used amassed data to keep older workers and women from seeing certain job postings.<sup>26</sup> Landlords have used data to keep racial minorities from viewing certain housing ads.<sup>27</sup> This outcome may occur as the result of discriminatory preferences or inadvertently as the result of the online advertising industry functioning as intended: Leigh Freund of the Network Advertising Initiative testified at these hearings that “women are less likely to see employment ads for careers in the science/technology/engineering/math field . . . simply because they have higher value to other advertisers because women do more shopping.”<sup>28</sup> If accurate, this demonstrates a market failure that threatens to deprive women of opportunities and employers of talented would-be employees.

Data-driven advertising also incentivizes the collection of more data, jeopardizing privacy. Moreover, the data demonstrate that, although some people generally like targeted advertising, they find the most privacy-intrusive ads “unnerving.”<sup>29</sup> The authors of a paper presented at the Thirteenth Symposium on Usable Privacy and Security found that more than half of participants feel negatively about behavioral targeted advertising, particularly when it is interest-based.<sup>30</sup> An article in the *Journal of Advertising* suggests that ads that are perceived to be too personal can seem intrusive and lower click-through rates and purchases.<sup>31</sup>

Against this backdrop, witnesses during the three days of FTC hearings on Big Data, Privacy, and Competition presented conflicting stories about the efficacy of behavioral advertising and consumers’ privacy preferences. Other witnesses discussed effective examples of privacy-by-design, and still others spoke of the externalities associated with big data.

---

<sup>25</sup> E.g. CAL. CIV. CODE § 1798.135(o)(1).

<sup>26</sup> See UPTURN, LEVELING THE PLATFORM: REAL TRANSPARENCY FOR PAID MESSAGES ON FACEBOOK (May 2018).

<sup>27</sup> Julia Angwin, Ariana Tobin, and Madeleine Varner, *Facebook (Still) Letting Housing Advertisers Exclude Users By Race*, PROPUBLICA, Nov. 21, 2017.

<sup>28</sup> Leigh Freund, President and CEO, Network Advertising Initiative, Competition and Consumer Protection Issues in Online Advertising, Testimony before the FTC Hearings on Big Data, Privacy, and Competition (Nov. 7, 2018).

<sup>29</sup> Michal Wlosik & Maciej Zawadzinski, *What is Contextual Targeting and How Does It Work?*, ClearCode, <https://clearcode.cc/blog/contextual-targeting/> (last visited Dec. 13, 2018).

<sup>30</sup> Sonam Samat, Alessandro Acquisiti, & Linda Babcock, *Raise the Curtains: The Effect of Awareness About Targeting on Consumer Attitudes and Purchase Intentions*, SOUPS 2017, <https://www.usenix.org/system/files/conference/soups2017/soups2017-samat-awareness.pdf>.

<sup>31</sup> Sophie C. Boerman, Sanne Kruijkemeier, & Frederik J. Zuiderveen Borgesius, *Online Behavioral Advertising: A Literature Review and Research Agenda*, 46 J. OF ADVERTISING 363, 372 (2017).

## *Data Does Not Demonstrate Behavioral Advertising's Superiority*

Leigh Freund of the Network Advertising Initiative testified that behavioral advertisements are perceived as more valuable than contextual advertisements.<sup>32</sup> Behavioral advertisements may be perceived as more valuable, but it is not clear that the available data demonstrate that they are more valuable. For example, Professor Florian Zettelmeyer testified that “many people [in the advertising industry] who spend a ton of money on marketing . . . simply do not know how well . . . [it is] working, because unless you plan ahead big-time and spend lots of money on doing randomized control trials, you literally have no sense of being able to tell whether your expenditures are actually working or not.”<sup>33</sup> He referenced a number of studies that both over- and under-estimate “lift” from behavioral advertising and explained that the online advertising industry does not have “a strong . . . tradition of very good measurement.”<sup>34</sup> Moreover, he reminded the FTC that the measurement of effective behavioral advertising should not be whether “it creates a lot of clicks,” but rather “whether it creates more clicks than you what would have happened had you not done whatever you did.”<sup>35</sup>

On the same panel, Professor Alessandro Acquisti testified that while behavioral advertisements are “500 percent times as expensive” as contextual advertisements, they only increase revenues by \$0.0008 per advertisement.<sup>36</sup> Moreover, he cautioned that advertising metrics are often inflated and, moreover, like Professor Zettelmeyer, he reminded the audience that advertising metrics can only measure so much – what if consumers would have bought the product or viewed the content even if they had not seen the advertisement? Was the advertisement still effective?<sup>37</sup>

Another area where the metrics may not match the common perception is the effect of data privacy regulation on innovation, as measured by investment. Garrett Johnson of Boston University’s Questrom School of Business testified that although Europe saw a twelve percent reduction in third party investment in the days leading up to GDPR’s effective date, that reduction bounced back up in certain countries and “by now are essentially where they were pre-GDPR levels.”<sup>38</sup>

---

<sup>32</sup> Leigh Freund, President and CEO, Network Advertising Initiative, Competition and Consumer Protection Issues in Online Advertising, Testimony before the FTC Hearings on Big Data, Privacy, and Competition (Nov. 7, 2018).

<sup>33</sup> Florian Zettelmeyer, Nancy L. Ertle Professor of Marketing, Kellogg School of Management, Northwestern University, The Economics of Big Data and Personal Information, Testimony before the FTC Hearings on Big Data, Privacy, and Competition (Nov. 6, 2018).

<sup>34</sup> *Id.*

<sup>35</sup> *Id.*

<sup>36</sup> Alessandro Acquisti, Professor of Information Technology and Public Policy, Heinz College, Carnegie Mellon University, The Economics of Big Data and Personal Information, Testimony before the FTC Hearings on Big Data, Privacy, and Competition (Nov. 6, 2018).

<sup>37</sup> *Id.*

<sup>38</sup> Garrett Johnson, Boston University Questrom School of Business, Economics of Online Advertising, Testimony before the FTC Hearings on Big Data, Privacy, and Competition (Nov. 7, 2018).

## *Consumer Preferences*

Notwithstanding the assertions that consumers’ “revealed preference[s]” suggest that they “don’t care enough about the tracking kinds of privacy concerns to be willing to do anything about it,”<sup>39</sup> witness after witness presented compelling evidence not only that consumers’ preferences and behavior align, but also that they demonstrate a deep concern for privacy.

For example, ninety-two percent of Facebook users change the social network’s default privacy settings.<sup>40</sup> This strongly suggests that consumers wish to preserve their privacy by choosing which audiences they share information with – and, indeed, they believe that they are limiting the audiences for their posts.

In terms of public opinion, “[n]inety-two percent of Americans think companies should have to get permission before sharing or selling their online data and 92 percent of Americans think companies should be required to give consumers a list of all the data they have collected about them.”<sup>41</sup> Those opinions are borne out in individuals’ behaviors. Julie Brill testified that more individuals in the United States use Microsoft’s dashboard to access their own data than Europeans do.<sup>42</sup> In addition, “it’s much harder to get people to fill out surveys than it used to be.”<sup>43</sup> Similarly, fewer people answer their cell phones today “if it’s an unrecognized number.”<sup>44</sup> Another witness posited that if consumers “don’t feel that their data are safe, they may not download apps on their phone . . . They may shut off Facebook or never post their child online because they don’t feel that privacy is protected.”<sup>45</sup> She suggested that there are costs associated with the slower adoption of technology that results from consumers’ privacy concerns. For example, because of privacy concerns, the U.S. has been slower to adopt electronic medical records, leading to “greater mortality, greater infant mortality.”<sup>46</sup>

---

<sup>39</sup> Howard Beales, Professor of Strategic Management and Public Policy, George Washington University, Competition and Consumer Protection Issues in Online Advertising, Testimony before the FTC Hearings on Big Data, Privacy, and Competition (Nov. 7, 2018).

<sup>40</sup> Emil Protalinski, *13 million US Facebook users don’t change privacy settings*, ZDNet, May 3, 2012, <https://www.zdnet.com/article/13-million-us-facebook-users-dont-change-privacy-settings/>.

<sup>41</sup> Christopher Boone, Vice President of Real World Data and Analytics, Pfizer, The Business of Big Data, Testimony before the FTC Hearings on Big Data, Privacy, and Competition (Nov. 6, 2018).

<sup>42</sup> Julie Brill, Corporate Vice President and Deputy General Counsel for Global Privacy and Regulatory Affairs, Microsoft, Former Enforcers Perspective: Where Do We Go From Here? What is Right, Wrong, or Indeterminate about Data Policy?, Testimony before the FTC Hearings on Big Data, Privacy, and Competition (Nov. 8, 2018).

<sup>43</sup> Avi Goldfarb, Rotman Chair in Artificial Intelligence and Healthcare, Rotman School of Management, University of Toronto, The Impact of Privacy Regulations on Competition and Innovation, Testimony before the FTC Hearings on Big Data, Privacy, and Competition (Nov. 7, 2018).

<sup>44</sup> Lior Strahilevitz, Sidley Austin Professor of Law, University of Chicago Law School, The Impact of Privacy Regulations on Competition and Innovation, Testimony before the FTC Hearings on Big Data, Privacy, and Competition (Nov. 7, 2018).

<sup>45</sup> Amalia Miller, Associate Professor of Economics, University of Virginia, The Impact of Privacy Regulations on Competition and Innovation, Testimony before the FTC Hearings on Big Data, Privacy, and Competition (Nov. 7, 2018).

<sup>46</sup> *Id.*

Where individuals are not selecting the most privacy enhancing options, there may be explanations aside from apathy. For example, Professor Rahul Telang testified that “people care if something goes wrong with their . . . credit card, with the bank, with something that has direct money involved, [sic] they are a lot more careful. On the other hand, if Home Depot loses your data or if Target loses your data . . . [o]ur transaction behavior doesn’t change a whole lot maybe because we think that, well, Lowe’s isn’t going to be any better. Maybe we think that the financial cost is really not very high, the credit card is going to pick it up, I’ll get a new credit card . . .”<sup>47</sup> Each of the explanations for consumer behavior that Professor Telang posited has little to do with consumer apathy about privacy and more to do with consumers’ resignation that companies are unwilling or unable to safeguard data in the digital age.<sup>48</sup>

Moreover, in some cases, businesses themselves have made it more difficult to select the most privacy enhancing options. For example, the advertising industry has, deliberately, it seems, made it unnecessarily difficult to understand – much less opt-out of – targeted advertising. The Future of Privacy Forum investigated which icon and associated phrase were most likely to convey to consumers that clicking on the icon/phrase would lead to disclosure information and options about behavioral advertising.<sup>49</sup> The Future of Privacy Forum found that the “asterisk man” icon and the phrases “Why did I get this ad?” and “Interest based ads” performed best. The phrase “Adchoice” performed noticeably less well.<sup>50</sup> The ad industry selected, instead of “asterisk man,” a small “forward I” icon and the phrase AdChoices.<sup>51</sup> This can only be interpreted as a cynical attempt to hide pertinent information from consumers. Given that the advertising industry has made it difficult and confusing for individuals to opt-out of targeted advertising, it is disingenuous to suggest that the paucity of opt-outs means people do not care about privacy. It is more likely that they cannot figure out how to navigate a deliberately difficult system.

### *Effective Privacy-by-Design*

Even as witness after witness presented evidence that call into question the value-add of big data and behavioral advertising and that underscored consumers’ genuine interests in privacy, other witnesses presented evidence of effective privacy-by-design.

For example, Mark MacCarthy of the Software & Information Industry Association testified that while “[s]ometimes you need a large data set to get the result[,] . . . these effects of size diminish after a certain point and you can add more data to the data set and you do not get

---

<sup>47</sup> Rahul Telang, Professor of Information Systems and Management, Carnegie Mellon University, The Impact of Privacy Regulations on Competition and Innovation, Testimony before the FTC Hearings on Big Data, Privacy, and Competition (Nov. 7, 2018).

<sup>48</sup> Professors Telang and Miller’s talks underscore the importance of securing communications networks in particular given that many uses of data, such as banking and electronic health records, rely on secure electronic transmission. *See generally* HAROLD FELD, CHARLES DUAN, JOHN GASPARINI, TEENYSON HOLLOWAY, & MEREDITH ROSE, PROTECTING PRIVACY, PROMOTING COMPETITION: A FRAMEWORK FOR UPDATING THE FEDERAL COMMUNICATIONS COMMISSION PRIVACY RULES FOR THE DIGITAL WORLD (Public Knowledge, 2016).

<sup>49</sup> *See* FPF Staff, *Online Behavioral Advertising “Icon” Study*, FUTURE OF PRIVACY FORUM (Feb. 15 2010), <https://fpf.org/2010/02/15/online-behavioral-advertising-icon-study/>.

<sup>50</sup> *See id.*

<sup>51</sup> *See* Jonathan Mayer, *Tracking the Trackers: The AdChoices Icon*, STANFORD LAW SCHOOL: THE CENTER FOR INTERNET & SOCIETY (Aug. 18, 2011), <http://cyberlaw.stanford.edu/blog/2011/08/tracking-trackers-adchoices-icon>.

anything new. So there are diminishing returns.”<sup>52</sup> Marianela Lopez-Galdos from the Computer and Communications Industry Association concurred, explaining that the value of data is limited. For example, if as soon as a consumer purchases a car, the value of the data generated from his or her car search becomes essentially useless.<sup>53</sup> Even Leigh Freund of the Network Advertising Initiative testified that data are relevant for thirty days or less.<sup>54</sup> This strongly suggests that a strict data deletion requirement could be privacy-enhancing without compromising multiple industries’ interests in those data.

There are also business models that thrive without collecting or monetizing consumer data. For example, Liz Heier testified that Garmin does not sell customer data. The majority of its products can be used without connecting to the internet. “[A]ll sharing options are set to private by default.” Garmin users can delete their data, and Garmin does not “constantly track the location of every Garmin device . . .”<sup>55</sup> In a very different line of business, Mastercard also successfully employs privacy-by-design. It only gets “enough data to process a payment.” It does not “need your name to process a transaction . . . [or] what you actually buy.”<sup>56</sup>

Finally, Professor Telang reminded the audience that there “are some other ways people are willing to pay [besides with their data or their dollars], including market share, transactions, how long we want to have a relationship with the firm . . .”<sup>57</sup>

In sum, testimony cast doubt on whether the most privacy-invasive practices actually increase return on investment for companies, it confirmed that consumers care deeply about privacy, and it presented examples of feasible privacy- and profit-enhancing corporate practices.

### *Externalities*

In addition to the foregoing takeaways, witnesses also presented compelling testimony about externalities that make clear that individuals and corporations cannot responsibly make privacy decisions in isolation. At the most basic level, “consumers often don’t know about all the problems that can arise, whether it’s on a data security side or on a privacy side . . .”<sup>58</sup> Moreover,

---

<sup>52</sup> Mark MacCarthy, Senior Vice President for Public Policy, Software & Information Industry Association, The Business of Big Data, Testimony before the FTC Hearings on Big Data, Privacy, and Competition (Nov. 6, 2018).

<sup>53</sup> Marianela Lopez-Galdos, Director of Competition & Regulatory Policy, Computer and Communications Industry Association, The Business of Big Data, Testimony before the FTC Hearings on Big Data, Privacy, and Competition (Nov. 6, 2018).

<sup>54</sup> Leigh Freund, President and CEO, Network Advertising Initiative, Competition and Consumer Protection Issues in Online Advertising, Testimony before the FTC Hearings on Big Data, Privacy, and Competition (Nov. 7, 2018).

<sup>55</sup> Liz Heier, Director of Global Data Privacy, Garmin, The Business of Big Data, Testimony before the FTC Hearings on Big Data, Privacy, and Competition (Nov. 6, 2018).

<sup>56</sup> Andrew Reiskind, Senior Vice President for Data Policy, MasterCard Worldwide, The Business of Big Data, Testimony before the FTC Hearings on Big Data, Privacy, and Competition (Nov. 6, 2018).

<sup>57</sup> Rahul Telang, Professor of Information Systems and Management, Carnegie Mellon University, The Impact of Privacy Regulations on Competition and Innovation, Testimony before the FTC Hearings on Big Data, Privacy, and Competition (Nov. 7, 2018).

<sup>58</sup> Lior Strahilevitz, Sidley Austin Professor of Law, University of Chicago Law School, The Impact of Privacy Regulations on Competition and Innovation, Testimony before the FTC Hearings on Big Data, Privacy, and Competition (Nov. 7, 2018).

the harms that stem from privacy abuses are often “greater than the harm to the[] individuals” involved.<sup>59</sup> For example, Cambridge Analytica used individuals’ data to distort democracy, “to make political lies more effective.”<sup>60</sup> The Strava fitness app exposed the locations of U.S. military outposts “outside Niger or in Afghanistan or places like this, [which is] not good for national security or for the group as a whole.”<sup>61</sup> Professor Omri Ben-Shahar compared the sorts of externalities produced by individuals’ privacy decisions to the sorts of externalities produced by individuals’ decisions around environmental pollution. Private “[c]ontracts, of course, are not going to solve the problem of externality.”<sup>62</sup> Just as regulation was necessary to limit the worst environmental damage, regulation is necessary to curtail the societal harms that arise from the use and misuse of data. Individuals and corporations are simply not equipped to make the best decisions for society as a whole.

## **5. Are there policy recommendations that would facilitate competition in markets involving data or personal or commercial information that the FTC should consider?**

While loud voices inside the advocacy community and elsewhere have called for stronger and more creative antitrust enforcement in markets involving data or personal or commercial information,<sup>63</sup> it is Public Knowledge’s view that, although antitrust has a role to play in protecting competition and consumer privacy in the digital age,<sup>64</sup> there are many important privacy problems that cannot be solved by antitrust. First, competition may create incentives to differentiate by providing greater privacy protections, but it could just as easily promote more intense efforts to obtain more personal data as a competitive edge. Second, any settlement after an investigation or consent decree as part of a merger approval can only be a primary tool for protecting privacy if thoroughly enforced on an ongoing basis, which would also require substantial FTC resources. Antitrust authorities often prefer structural remedies such as divestiture of assets to shrink market power, rather than remedies that require them to regulate the conduct of companies in the marketplace on an ongoing basis. Third, antitrust action may just turn one privacy offender monopolist into several privacy offender competitors. Finally, the consequences and impacts of a privacy violation can be the same regardless of the size of the company involved, but in most cases, antitrust cannot remedy most privacy harms caused by non-dominant players, which may be just as damaging to consumers as the same conduct by a dominant player.

However, there are several actions the FTC – and the federal government more broadly – can take to promote privacy and competition in the digital age. Narrowly, under its antitrust purview, the FTC should use antitrust to encourage nonprice competition, including competition based on different levels of privacy protection. Antitrust law should recognize that one of the

---

<sup>59</sup> Omri Ben-Shahar, Leo and Eileen Herzel Professor of Law and Keaarny Director of the Coase-Sandor Institute for Law and Economics, University of Chicago Law School, *The Economics of Big Data and Personal Information*, Testimony before the FTC Hearings on Big Data, Privacy, and Competition (Nov. 6, 2018).

<sup>60</sup> *Id.*

<sup>61</sup> *Id.*

<sup>62</sup> *Id.*

<sup>63</sup> E.g. Allen P Grunes and Maurice E Stucke, *No Mistake About It: The Important Role of Antitrust in the Era of Big Data* (Univ. of Tenn. L. Studies Research Paper No. 269), <https://papers.ssrn.com/abstract=2600051>.

<sup>64</sup> See Eugene Kimmelman, Harold Feld, & Agustin Rossi, *The limits of antitrust in privacy protection*, INT’L DATA PRIVACY L. 8, 270 (2018).

harms of market dominance may be the power to coerce consumers into providing personal information in return for products or services with few or no competitors.<sup>65</sup> In addition, the possession of personal data, particularly large amounts of aggregated data, could be considered as a potential barrier to entry during merger review, even when a merger would not otherwise have significant vertical or horizontal competitive effects.

The FTC could also use its unfair and deceptive practices authority to explore, through case-by-case adjudication whether it is deceptive for websites and services to place third party trackers all over the internet, tracking even those who do not have accounts with those websites and services.

And, the FTC could conduct a 6(b) study of how platforms are using data and how their data use effects competition. Platforms have the advantage of setting the rules of the game on their platforms. Unsurprisingly, they have claimed valuable transaction, voice command, search, user, and advertiser data for themselves. This entrenches their advantages and may create a barrier to entry to potential competitors. Platforms may be making purposeful choices to enhance this advantage. It is not clear to the public what is happening in this space, or whether any violations have occurred. The advantage of a 6(b) study is that it results in a public, published report. This way, if the solution to big data, privacy, and competition problems is not – or is not entirely – antitrust, the FTC and the public will have the background needed to pursue other solutions.

Specifically in the context of online advertising, the topic that consumed much of the three days of hearings, a more privacy-enhancing approaches would actually be more competition-enhancing. Reliance primarily on behavioral advertising is likely to entrench the duopoly of players with access to vast troves of consumer data, and consumers are likely to sacrifice even more privacy as they and their would-be competitors strive to scoop up more and more personal information. However, if Congress were to limit data use for advertising, the US might see a return to contextual advertising<sup>66</sup> – for example, advertising on ESPN to reach sports fans and in Rolling Stone to reach music fans – a practice that is more privacy-protective because an advertiser need not know everything about a consumer, that many more can engage in, and that may have benefits for advertisers.

Contextual advertising is significantly less expensive for advertisers. For example, Professor Alessandro Acquisti testified that while behavioral advertisements are “500 percent times as expensive” as contextual advertisements, they only increase revenues by \$0.0008 per advertisement.<sup>67</sup> In addition, contextual advertising is helpful from a brand-safety perspective,

---

<sup>65</sup> See generally HAROLD FELD, CHARLES DUAN, JOHN GASPARINI, TEENYSON HOLLOWAY, & MEREDITH ROSE, PROTECTING PRIVACY, PROMOTING COMPETITION: A FRAMEWORK FOR UPDATING THE FEDERAL COMMUNICATIONS COMMISSION PRIVACY RULES FOR THE DIGITAL WORLD (Public Knowledge, 2016).

<sup>66</sup> Cf. Orla Lynskey, Associate Professor of Law, London School of Economics and Political Science, The Potential Impact of GDPR on Competition and Innovation, Testimony before the FTC Hearings on Big Data, Privacy, and Competition (Nov. 7, 2018) (explaining that GDPR implementation will push Europe toward contextual advertising).

<sup>67</sup> Alessandro Acquisti, Professor of Information Technology and Public Policy, Heinz College, Carnegie Mellon University, The Economics of Big Data and Personal Information, Testimony before the FTC Hearings on Big Data, Privacy, and Competition (Nov. 6, 2018).

because placing ads in context makes it more likely that they will not appear next to problematic content.<sup>68</sup>

Finally – and relatedly – the FTC should advocate with Congress for passage of a comprehensive privacy law that would imbue the agency with much-needed resources and empower it with rulemaking authority.<sup>69</sup> This is not a novel idea: the “golden age” of trust busting in the first half of the 20th century also saw the first wave of comprehensive consumer protection law.<sup>70</sup>

In all of its actions, the FTC should remember that while innovation and competition are important, they are means to an end rather than ends in themselves. For example, while there is insufficient competition in the pharmaceutical industry, as a society, the United States has decided not to permit unsavory characters to sell snake oil on the sidewalk. Such salespeople might increase competition in the pharmaceutical industry and might reduce prices, but would do so at the expense of public welfare. Similarly, the role of regulation is, at least in part, to prevent unsavory entities that would misuse, abuse, and fail to safeguard consumers’ data from entering the market in the name of competition and innovation.

## **Conclusion**

We were grateful for the opportunity to testify at the Federal Trade Commission’s Hearings on Competition and Consumer Protection in 21st Century: Big Data, Privacy, and Competition, and we appreciate the opportunity to submit these comments, in response to Docket ID: FTC-2018-0100, reflecting on the hearings.

Sincerely,



Allison S. Bohm  
Policy Counsel  
Public Knowledge

---

<sup>68</sup> See generally Press Release, 4A’s, 4A’s Advertiser Protection Bureau Delivers Brand Suitability Framework and Brand Safety Floor in Move to Help Advertisers Assess Risk (Sept. 20, 2018) (<https://www.aaa.org/4as-advertiser-protection-bureau-delivers-brand-suitability-framework-and-brand-safety-floor-in-move-to-help-advertisers-assess-risk/>).

<sup>69</sup> For a discussion of what such legislation should include, see generally Letter from Allison S. Bohm, Policy Counsel, Public Knowledge, to Senator John Thune, Chairman, Senate Committee on Commerce, Science, and Transportation and Senator Bill Nelson, Ranking Member, Senate Committee on Commerce, Science, and Transportation (Oct. 10, 2018) (<https://www.publicknowledge.org/documents/pk-statement-for-senate-commerce-hearing-on-consumer-data-privacy>); see also Letter from Allison S. Bohm, Policy Counsel, Public Knowledge, to David J. Redl, Assistant Secretary for Communications and Information, Nat’l Telecomm. & Info. Admin. (Nov. 9, 2018) (<https://www.publicknowledge.org/documents/public-knowledge-ntia-consumer-privacy-comments>).

<sup>70</sup> Gene Kimmelman & Mark Cooper, *A Communications Oligopoly on Steroids - Why Antitrust Enforcement and Regulatory Oversight in Digital Communications Matter*, WASHINGTON CENTER FOR EQUITABLE GROWTH, Jul. 2017, <https://live-equitablegrowth.pantheonsite.io/wp-content/uploads/2017/07/071817-kimmelman-cooper2.pdf>.