

*Comments submitted to the Federal Trade Commission in the Matter of:*

# HEARING ON COMPETITION AND CONSUMER PROTECTION IN THE 21<sup>ST</sup> CENTURY

## The Consumer Welfare Implications Associated With the Use of Algorithmic Decision Tools, Artificial Intelligence, and Predictive Analytics

**Ryan Hagemann**  
Senior Director for Policy  
Niskanen Center

Submitted: August 20, 2018  
Docket Number: FTC-2018-0056

---

## EXECUTIVE SUMMARY

Artificial intelligence and (AI) and machine learning (ML) are potentially transformative technologies that could herald considerable economic gains across the entire American economy. From advancements in medical technologies to improved online user experiences and new innovative commercial applications, AI/ML is already at the forefront of driving consumer welfare benefits in numerous sectors of economic and social life.

As AI/ML technologies continue to play an increasingly important role in promoting substantial gains in consumer welfare, concerns regarding automated decision-making and the privacy implications of those decisions will continue challenging the beneficial applications of AI/ML. In order to address those specific harms that do materialize, the FTC should embrace a regulatory framework that can better balance the needs of innovators, consumer expectations, and privacy concerns. These comments recommend a framework for “algorithmic accountability,” which has the benefit of being a technologically-neutral approach to governing automated decision-making without requiring new laws or rules to address the potential harms resulting from advancements in AI/ML.

In addition to recognizing and implementing “algorithmic accountability,” the FTC should consider the following recommendations as it moves forward with its proposed hearings:

1. Avoid attempting to address the issue of pricing or quantifying the value of data, and, by extension, refrain from considering claims of “data price gouging” as constituting anticompetitive practices;
2. Consider how recent advancements in AI/ML have helped contribute to better understanding the return on investment for digital advertising and investment, and the implications for assessing gains to consumer welfare;
3. Examine how implementing specific rules for “algorithmic accountability” could address potential harms in sector-specific contexts; and
4. When considering “purposes specification” rules for data, data retention mandates, or default opt-in requirements, the FTC should give considerable weight to evidence detailing the economic costs associated with such proposals.

# INTRODUCTION

At its core, artificial intelligence (AI) is a technology that simply improves outcomes by offloading specific tasks to software — tasks that are better suited for computers to handle. Machine learning (ML) is the process by which statistical models allow AI systems to improve their outputs and decisions based on data inputs. In other words, ML is the process by which data drives learning in AI systems, which is why large diverse data sets are so integral to the process of improving these technologies.

As an example of AI/ML at work in the real world, consider how the effectiveness of IBM’s Watson software system is constantly evolving and improving. Watson is a natural language processing system, which means it can understand questions and respond with a relatively high degree of accuracy. It is capable of performing these tasks, and improving itself, through a process of anfractuous data input/output analysis. Watson “ingests” information from human-curated data sets and then creates indexes to differentiate the types of data in its “library” (e.g., distinguishing medical journals from U.S. presidents). Then, the ML process is primed to begin learning from real-world experience. In a very general sense, that learning and improving occurs as follows: (1) the system identifies the specific parts of speech in a question; (2) it then generates inquiries/hypotheses as to the likely context; (3) evidence is sought to either affirm or refute those hypotheses; and (4) it scores that evidence based on statistical modeling to arrive at an answer that satisfies the original question. This technology is still in its early stages, and while AI systems can occasionally resemble human-level decision-making, such systems bear only superficial resemblance to true “thinking” and “thought.”

With those limitations in mind, the comments that follow are tailored with an eye towards discussing the specific welfare-enhancing benefits of AI/ML. Because of the extent of this technology’s impact, however, the discussion will necessitate occasional deviations into the broader realm of the online digital economy. It is in this ecosystem — in particular, the Internet, online service providers/platforms (OSP), and the digital advertising industry that forms its economic backbone — where AI/ML is likely to have the most immediate impact on consumer welfare, industry competition, and American innovation more generally. As a result, these comments will focus on the following two questions from the Federal Trade Commission’s (FTC) request for comment on the consumer welfare implications associated with AI/ML:

1. The welfare effects and privacy implications associated with the application of these technologies to consumer advertising and marketing campaigns; and
2. Whether restrictions on the use of computer and machine learning and data analytics affect innovation or consumer rights and opportunities in existing or future markets, or in the development of new business models.

Part I will begin with a more general discussion of how consumers view the issue of privacy in the context of online services in the digital age, followed by a brief discussion of how the digital advertising market works. It will then summarize the consumer welfare gains from commercial applications of AI/ML to this market.

Part II will examine the particularly problematic provisions of the EU’s new General Data Protection Regulation (GDPR), the recently-enacted California Consumer Privacy Act of 2018 (CCPA), and compare the purported value and effectiveness of these far-reaching approaches to regulating privacy with existing self-regulatory mechanisms and frameworks. It will conclude by looking at how the various provisions and regulatory approaches will likely impact AI/ML investment and commercial applications, as well as innovation, consumer welfare, and competition in the broader digital economy. Finally, Part III summarizes

a set of recommendations that can help guide the FTC as it considers policies that can equitably balance the complex web of trade-offs implicated by ongoing developments in, and applications of, AI/ML technologies.

## **PART I: CONSUMER WELFARE & PRIVACY**

### **EFFECTS OF INTEGRATING AI INTO DIGITAL MARKETS**

In 2001 testimony before the House Subcommittee on Commerce, Trade and Consumer Protection, the famed privacy scholar Alan Westin noted that despite privacy concerns, “American consumers, by large majorities, want all the benefits and opportunities of a consumer service society and of a market-driven social system.”<sup>1</sup> Based on a catalog of research and direct experience with dozens of national privacy surveys going back to 1979, Westin’s analysis concluded that Americans were wary of broad-based privacy regulations. As he testified:

*We know that a majority of the American public does not favor the European Union style of omnibus national privacy legislation and a national privacy regulatory agency, but when it comes to sensitive information such as financial information or health information, overwhelming majorities are looking to legislative protections to set the rules and the standards for that kind of activity.<sup>2</sup>*

In the 17 years since Westin noted the public’s attitudes towards “omnibus national privacy legislation,” much has changed; but consumer privacy preferences continue to show the same skepticism towards broad, baseline rules that may imperil access to cheap or zero-priced online services.

#### **A. Privacy Preferences in the Digital Age**

The issue of privacy has increasingly become a flashpoint of technology policy debates. These emotional eruptions are primarily the result of a belief that privacy is a human right — one that occupies so profound a position in the constellation of human values that it is innately inalienable and should never be subject to commodification, regardless of the potential social or economic benefits.<sup>3</sup> Since the early-1990s, numerous “Privacy Fundamentalist”<sup>4</sup> organizations have emerged to advocate on behalf of this position.<sup>5</sup> Although these voices tend to be louder and more emotionally forceful than others, the shrillness with which a conviction is proclaimed is not dispositive of some manifest truth; merely disputing the *absolute* sacrosanctity of privacy does not imply a cavalier indifference to its value.

Indeed, as Eli Noam, professor of finance and economics at Columbia University, acknowledges, one can recognize the importance of privacy rights while also weighing its value relative to other considerations:

*To state that privacy is a basic human right is a noble sentiment with which I am in accord, but it does not follow that privacy therefore is outside the mechanism of transactions. As mentioned, a right is merely an initial allocation. It may be acquired without a charge and be universally distributed regardless of wealth, but is in the nature of humans to have varying preferences and needs, and to exchange what they have for what they want. Thus, whether we like it or not, people continuously trade in rights. In doing so they exercise a fundamental right, the right of free choice.<sup>6</sup>*

Noam is not alone in this perspective. In fact, the majority of the academic literature on the economics of privacy treats the issue in a much more balanced and nuanced way than the Privacy Fundamentalist outlook. As Alessandro Acquisti, Curtis Taylor, and Liad Wagman noted in a recent journal article summarizing this literature:

*Extracting economic value from data and protecting privacy do not need to be antithetical goals. The economic literature we have examined clearly suggests that the extent to which personal information should be protected or shared to maximize individual or societal welfare is not a one-size-fits-all problem: the optimal balancing of privacy and disclosure is very much context dependent, and it changes from scenario to scenario. In fact, privacy guarantees may be most needed precisely when the goal is to extract benefits from the data. ... Thus, it stands to reason that, case by case, diverse combinations of regulatory interventions, technological solutions, and economic incentives, could ensure the balancing of protection and sharing that increases individual and societal welfare.<sup>7</sup>*

This view of privacy — as a complicated balancing act between many different values — is not just shared by academics and researchers, but tends to be the prevailing view of average consumers on both sides of the Atlantic. Despite assumptions regarding the high premium Europeans place on laws and regulations protecting privacy and de-prioritizing data collection, perceptions of responsibility suggest otherwise. Indeed, a 2011 survey report from the European Commission indicated that:

*Respondents who use social networking or sharing sites were asked who they think should make sure that their information is collected, stored and exchanged safely on these sites. ... Initially, half of the respondents point to themselves (49%), while one-third point to the social networking or sharing sites (33%). Even fewer identify the public authorities (16%). ... When the interviewees are given the opportunity to name a second responsible entity or person, the total results mention social networking or sharing sites (73%) and the respondents themselves (74%) almost equally; public authorities are cited much less (45%).<sup>8</sup>*

That same survey also detailed how for younger Europeans in particular, disclosing personal information in exchange for zero-price online services was “not a big issue” and they felt “[sufficiently informed about the conditions for data collection and the further uses of their data when joining a social networking site or registering for a service online.”<sup>9</sup>

More generally, when looking at both surveys and behavioral studies asking the question of how much people value their privacy, the general conclusion that appears time and time again is: such decisions are complicated, contextual, and highly subjective. Behavioral experiments often conclude, among other things, that numerous factors have significant, sometimes contradictory, impacts on consumer choices regarding their personal valuation of privacy, including: the particular framing of default options for notice-and-consent terms of use,<sup>10</sup> the presence of “social desirability biases,”<sup>11</sup> and consumer price sensitivities towards privacy trade-offs.<sup>12</sup>

The take-away from all of this is that privacy is a complicated, multidimensional, and highly contextual bundle of preferences and interests. Separating the many elements that constitute an individual’s expectation of privacy is a notoriously difficult — and perhaps impossible — task; and attempting to aggregate all this information to create a more holistic picture of how consumers, as a group, broadly value privacy has thus far yielded little in the way of actionable insights. Privacy preferences are immensely atomistic, and very few conclusions can be drawn from these studies that would offer ideal one-size-fits-all solutions for society writ large.

## **B. The Digital Advertising Market and its Effects on Consumer Welfare**

Leaving privacy considerations aside for the moment, there is a wealth of evidence suggesting the use of OSPs result in significant gains to consumer welfare.

For example, a 2010 analysis from McKinsey & Company showed that consumer surplus, fueled by ad-funded Internet services, continues rising, with consumers reaping the lion's share (about 85 percent, with 15 percent going to producers) of total surplus value in 2010 (valued at approximately \$100 billion).<sup>13</sup> The report goes further, noting that “the price an Internet consumer is willing to pay to avoid [advertisement disturbances] is worth only one-sixth of the total value derived from ad-funded Web services.”<sup>14</sup> It continues:

*More than 80 percent of current Internet users generate significantly more value from using the Web than what they would be willing to pay to eliminate [advertising] disturbances. Further, what they would be willing to pay in total is less than current online advertising revenue, making the economic equation of Internet innovation unsustainable. As a result, any potential focus on reducing disturbance should be weighed against the risk of reducing ad-funded user innovations online.*<sup>15</sup>

Despite the dated nature of the report, there is an abundance of research papers, surveys, and behavioral experiments that all echo similar conclusions regarding the clear value consumers place on Internet use and digital services. For example, in a 2006 National Bureau of Economic Research working paper, Austan Goolsbee and Peter Klenow estimated that consumer surplus from Internet usage could be as much as 2 percent of an individual's full-income, amounting to potentially hundreds or thousands of dollars in benefits to consumers.<sup>16</sup> While it is certainly true that the difficulty of “pricing” an individual's data could be yielding an outsized share of benefits for OSPs and digital advertisers, consumers nonetheless reap considerable net positive benefits in welfare, creating a win-win situation for all involved.<sup>17</sup> Indeed, attempting to attach a clear price signal to data is an endeavor fraught with difficulty, if not impossibility, and is more likely to simply add additional confusion to the discussion of consumer welfare benefits resulting from the digital economy. Indeed, attempts at quasi-quantification of data-pricing are already being considered by certain European regulators to provide pseudo-empirical justifications for more expansive antitrust enforcement efforts against American technology firms.<sup>18</sup>

Instead of attempting to quantify a data-price or force non-empirical considerations of individual privacy preferences into the forthcoming hearings, the FTC should instead focus its attention on how the use of AI/ML can actually improve the digital ad auction ecosystem. As Joaquin Quinonero-Candela, Facebook's director of applied machine learning, noted in a 2013 article in the *Journal of Machine Learning Research*, “Ad placement decisions [on websites] impact the satisfaction of the users and therefore their willingness to frequent this web site in the future.”<sup>19</sup> The article goes on:

*Whenever a user visits a publisher web page, an advertisement placement engine runs an auction in real time in order to select winning ads, determine where to display them in the page, and compute the prices charged to advertisers, should the user click on their ad. Since the placement engine is operated by the publisher, it is designed to further the interests of the publisher. Fortunately for everyone else, the publisher must balance short term interests, namely the immediate revenue brought by the ads displayed on each web page, and long term interests, namely the future revenues resulting from the continued satisfaction of both users and advertisers.*<sup>20</sup>

This is an important, albeit implicit, recognition of the consumer welfare-enhancing effects of OSPs serving both advertisers as well as users. Because many OSPs function as two-sided markets, assessing the full extent of consumer welfare gains involves more nuance than in traditional one-sided markets.<sup>21</sup> However, as AI/ML technologies continue to improve programmatic ad buys, they will become an increasingly valuable means of optimizing the “short term interests” of users, as individuals receive better-targeted, and perhaps fewer, ads while continuing to enjoy zero-priced digital services.

## C. Summary

**What are the welfare effects and privacy implications associated with the application of these technologies to consumer advertising and marketing campaigns?**

By optimizing ad placements, tailoring content to individual customer expectations, and scaling those capabilities to reach wider audiences, AI/ML will benefit consumers, advertisers, and the wider digital ecosystem.<sup>22</sup> In fact, an overwhelming majority of bids in the online auction markets — approximately 80 percent by some estimates — are already made using narrow AI to make programmatic ad purchases, and that number is only expected to rise in the coming years.<sup>23</sup>

For consumers, these gains come in the form of more targeted and relevant advertisements, improving the user experience online without diminishing the quality of zero-priced services consumers have come to expect.

For digital advertisers, the benefits of deploying AI/ML are potentially much more profound. Every year, digital ad fraud — in particular, “invalid traffic” automated systems that artificially inflate the number of clicks, impressions, views, etc. with the aim of generating revenue for the perpetrators<sup>24</sup> — costs online advertisers billions of dollars, and continues to skyrocket. In 2015, a report commissioned by the Interactive Advertising Bureau found that digital ad fraud cost the industry \$8.2 billion, with invalid traffic comprising the largest segment of those costs (\$4.6 billion).<sup>25</sup> A 2017 report from Juniper Research forecasted that these costs could jump to \$19 billion in 2018.<sup>26</sup> While AI/ML technologies are likely being employed in the commission of ad fraud, they are also being harnessed as a potential solution. Existing systems, such as PPC Protect,<sup>27</sup> and forthcoming innovations, such as the NOIZ decentralized digital advertising platform,<sup>28</sup> promise to significantly curtail these costs, minimizing the deadweight losses for advertisers and diminished online experience for users.

## PART II: HOW AI REGULATIONS IMPACT INNOVATION & CONSUMER WELFARE

Of the top 25 global technology companies by total market capitalization, 15 are American firms with a combined total value of almost \$5 trillion. By contrast, Europe’s contribution to the global technology sector is three firms with a total market capitalization of \$285 billion.<sup>29</sup> To put that into a bit more context, Intel alone is almost as valuable as the entire European technology industry.

A primary reason for this gulf is the European regulatory burden, which tends to reduce the incentives for investments in productivity-enhancing technologies and complementary assets that contribute to modern economic growth. A 2013 working paper from the European Commission noted as much when it identified one of the primary hurdles inhibiting the continent’s tech sector was “the need for more competition in the product market,” and noted that “a higher level of regulation tends to be negatively correlated with the share of ICT investment over total investment and product market regulation,” which explains a significant amount of cross-country investment in information technologies.<sup>30</sup>

Between 2012 and 2016, the average U.S. venture capital exit was nearly \$200 million.<sup>31</sup> In Europe, the average was \$70 million. The total number of \$250 million exits during this five-year period? 166 in the United States, compared to only 22 across all of Europe. And Europe also lags on creating tech “unicorns,” producing only one-tenth the number as the United States does, in large part due to the Series C “black hole” for the European tech sector. At the current rate, Europe’s VC industry won’t arrive at current U.S. levels for

another three decades, which would, even by optimistic estimates, still only add upwards of \$100-150 billion of future economic value to the EU's tech industry.

This significant trans-Atlantic divide in investment and firm size/valuation has profound effects for the adoption of commercial AI/ML technologies and showcases the many costs associated with adopting more rigorous rules and regulations on the use of consumer data.

As a June 2017 McKinsey Global Institute analysis reported:

*Industries most likely to lead the adoption of AI technologies at scale are those with complex businesses in terms of both operations and geography, whose performance is driven by forecasting, fast and accurate decision making, or personalized customer connections. In financial services, there are clear benefits from improved accuracy and speed in AI-optimized fraud-detection systems, forecast to be a \$3 billion market in 2020 ... In retail, there are compelling benefits from improved inventory forecasts, automated customer operations, and highly personalized marketing campaigns. Similarly, in health care, AI-powered diagnosis and treatment systems can both save costs and deliver better outcomes for patients.<sup>32</sup>*

This section examines various existing, forthcoming, and proposed regulatory restrictions that either directly or indirectly implicate AI/ML technologies. Specifically, it will look at these rules in the context of the broader digital economy, where such technologies are most likely to have near-term economic impacts, and how innovation and consumer welfare are likely to be, or already are, affected.

The first subsection (“Existing Rules and Regulations”) provides an overview of how privacy and consumer data protection are currently governed by a variety of frameworks, both federal statutes and self-regulatory approaches. It will also detail provisions of rules like GDPR and CCPA, which vest greater responsibility for enforcing stricter privacy rules in the hands of the EU and California government, respectively. The subsequent subsection (“Other Proposed Rules and Regulations”) then addresses the issues associated with more specific regulatory mandates: “purpose specification” limitations, data retention specifications, and default opt-in requirements. It concludes by summarizing the impact all of these provisions have for AI/ML adoption in the digital economy.

## **A. Existing Laws, Regulations, and Governance Frameworks**

Privacy regulation in the United States has a long history of governing particularized harms materializing from specific types of information about individuals that — depending on the sensitivity of the data in question, and the *specific* harm implicated by its revelation, circulation, etc. — are afforded more or less stringent protection requirements. For example, healthcare and financial information are typically considered more sensitive than online browsing habits, and for good reason: an individual's credit card information, if unsecured, could result in unapproved charges, or in more extreme situations, identity theft.<sup>33</sup> In assessing the harms resulting from privacy violations, context matters — a lot.

While there are certainly valid criticisms of a more fractured approach to governing privacy, what such an approach lacks in the benefits of a unified framework it makes up for in striking an effective balance between innovation and competing privacy preferences. In one of the most comprehensive analyses of the costs and benefits of privacy rules for the digital ecosystem, a 2001 working paper from the AEI-Brookings Joint Center for Regulatory Studies authored by Robert W. Hahn and Anne Layne-Farrar, speaks to the value of a sector-based privacy regime:

*Complaints about the patchwork of regulations governing information privacy in the U.S. notwithstanding, there are valid reasons for supporting a selective approach to information privacy protection. Passing laws one at a time, for specific areas, allows for a more careful evaluation of issues. In principle, such laws are less prone to — although certainly not immune from — unintended consequences. This approach also allows (at least in theory) for lawmakers to consider the costs and benefits that each proposed act is likely to entail. After enough time for evaluation, those laws that are seen as not covering enough ground may be amended, as was the case with both the Electronic Communications Privacy Act and the Fair Credit Reporting Act. With the federal government, enacting legislation in an incremental fashion is easier than eliminating bad policy once it is on the books.<sup>34</sup>*

The following sections describe the current landscape of norms, oversight, and governance — beyond the FTC — that regulates the broader digital economy and applications of AI/ML that may implicate consumer welfare and privacy, both here in the United States and in the EU.

## I. The General Data Protection Regulation

As noted previously, GDPR has a direct bearing on the potential for a flourishing digital economy in Europe. In particular, a number of the rule's provisions directly or indirectly implicate how, and whether, firms might employ AI.

- **Article 13** obliges firms to provide individuals with information regarding the “purposes of the processing for which the personal data are intended”;<sup>35</sup>
- **Article 14** imposes a similar obligation on firms as noted under **Article 13**, but for information that was not obtained from the data subject directly;<sup>36</sup>
- **Article 15** reiterates many of the same rights under **Articles 13 and 14**, while further enshrining the right of individuals “to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed”;<sup>37</sup>
- **Article 17** stipulates that data subject may “obtain from the controller the erasure of personal data concerning him or her without undue delay;”<sup>38</sup> and
- **Article 22** affords the right to have “significant” algorithmic decisions reviewed by a human,<sup>39</sup> and stipulates specific standards by which “human intervention” is to be judged.<sup>40</sup>

**Articles 13, 14, and 15** collectively provide EU citizens with a “right to explanation,” **Article 17** grants a “right to erasure,” and **Article 22** confers a “right to review” decisions subject to automated decision-making systems, such as AI/ML.

In addition to the individual articles, GDPR also provides a series of 173 — non-binding supplemental expositions that provide guidance to judges attempting to interpret the law.<sup>41</sup> The very existence of such supplemental interpretations suggests the rules as written are so complex and difficult to interpret that additional guidance is required for the inevitable legal challenges that are likely to follow. Unfortunately, even this additional corpus of guidance offers little clarity on the more confusing provisions of the many GDPR clauses that implicate algorithmic decision-making. For example, the phrase “meaningful information about the logic involved” in algorithmic decision-making described in Articles 13, 14, 15, and 22, is lacking any precise meaning. As Nick Wallace and Daniel Castro of the Center for Data Innovation noted in a March 2018 report:

*The GDPR provides relatively little clarification as to how it defines “meaningful information” ... The articles themselves do not specify whether “meaningful information about the logic involved” refers to an explanation of how a particular algorithm generally reached decisions, or to a precise explanation of exactly how the algorithm arrived at a particular conclusion. Recital 71 seems to imply the latter when it says the data subject should be able to “obtain an explanation of the decision,” but it does not specify what information would constitute an explanation or whether information about the “logic involved” should pertain to the algorithm or to the decision.<sup>42</sup>*

The problematic provisions extend beyond these articles and recitals, however, as GDPR is vague regarding the standards by which de-identified data are judged, imposes a data-localization mandate by requiring companies to use EU-based data centers, and fails to make appropriate allowances for the difficulties inherent in its data portability directive.<sup>43</sup>

Taken together, the many provisions of GDPR and attendant recitals create a complicated web of impracticable obligations for firms and innovators seeking to deploy AI systems. The result is that no one truly knows what compliance looks like, creating wide-scale regulatory uncertainty for all but the largest incumbents with the resources to invest in large, well-rounded compliance teams and data protection and privacy officers.<sup>44</sup> This is not a recent problem. At least as far back as 1999, in the budding days of commercial Internet services, researchers noted that the then-privacy rules governing digital data in the EU — the EU Data Protection Directive — would have a similar impact on the continent’s digital economy in the years to come. As Peter Swire and Robert Litan wrote back in 1998, the Directive’s provisions suggested that there may be a “possibility that strict data protection rules in Europe, coupled with less strict rules in other countries, will pose a competitive disadvantage for Europe. The risk is that Europe will fall behind in creating the information society.”<sup>45</sup> And indeed, as the recent numbers regarding the investment and market capitalization gulf between the American and EU technology sectors very clearly indicate, Europe not only fell behind — it never even started running in the race.

Swire and Litan offered a solution to this problem, arguing that organizations transferring and processing data across national boundaries be permitted to regulate based on a set of self-imposed governance standards. While they recognized the inherent difficulties associated with transnational enforcement and oversight of such a system, they argued such concerns could potentially be overcome through the use of self-regulatory mechanism contracts, affirming data users are afforded “adequate” privacy protections while retaining the flexibility necessary for easing cross-border compliance.<sup>46</sup> Of course, no such system ever materialized, and the rigidity of the EU’s approach to governing privacy had negative competitive reverberations beyond its wilting Internet economy.<sup>47</sup>

While the purported intent of GDPR is to protect consumer privacy,<sup>48</sup> the trade-off is a regulatory ecosystem that entrenches incumbents and creates high entry barriers for new startups, diminishing the potential for future competition and effectively chilling the digital platform economy.<sup>49</sup> The costs to new market entrants have already been significant, with many European-based technology startups shuttering their doors in GDPR’s wake,<sup>50</sup> and digital ad revenues plummeting by up to 40 percent in some cases.<sup>51</sup> Additionally, the U.S. Chamber of Commerce estimated that once enacted, GDPR would cause significant net consumer welfare losses for European trade competitiveness, resulting from serious disruptions to cross-border data flows and online trade services.<sup>52</sup> In addition, the Chamber’s analysis estimated that under such a digital trade disruption scenario, the direct effect for consumer welfare could be a loss of \$1,353 for individual four-person EU households.<sup>53</sup> The analysis concludes by expressing the same perspective as the economics literature on privacy, noting “the need to evaluate the economic implications and the importance of seeking the least trade-restrictive measure for the objective sought. Regulations with severely trade-distorting effects often begin with the pursuit of legitimate goals, but they get clouded by a disregard for a balance between

objectives sought and restrictiveness imposed.”<sup>54</sup> Additionally, there is strong evidence to suggest that GDPR’s nebulous rules, high penalties for non-compliance, and broad discretionary enforcement authority are creating an environment in which EU regulatory action is increasingly coming to resemble capricious trans-Atlantic wealth transfers more than actions aimed at correcting genuine market failures.<sup>55</sup>

Despite this parade of horrors, GDPR-variants have been cropping up all over the world — most notably, and recently, in California.

## 2. The California Consumer Privacy Act

Like GDPR, the recently-passed CCPA includes numerous impracticable mandates, buttressed by exceptionally vague language and definitions. For instance, “personal information” is defined as “information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.”<sup>56</sup> This excludes “deidentified information,” which is defined as “information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer.”<sup>57</sup> The definition of “aggregate consumer information” suffers from a similar lack of clarity, defined as “information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device.”<sup>58</sup>

These broad definitions create problematic issues when attempting to interpret the extent of the law’s reach. For example, as Santa Clara University law professor Eric Goldman has noted, the inclusion of “olfactory information” as a type of personal information implicated by CCPA means that, “in theory, when an employee passively smells a customer in the ordinary course of business (if you’ve ever worked retail, you know exactly what I’m talking about), this would constitute a “collection” that needs to be disclosed and would possibly trigger other obligations.”<sup>59</sup> The expansive nature of these definitions is so pronounced that even CCPA’s own supporters explicitly recognize issues of its feasibility.<sup>60</sup> The fundamental problem of such expansive and overly-inclusive language is that it fails to distinguish between sensitive and non-sensitive types of information while subjecting all businesses to the same costly compliance costs. As Goldman notes, the initiative that drove CCPA’s passage

*was marketed as a way of curbing the excesses of the Internet giants like Google and Facebook. While the law certainly applies to them, the law treats the local pizza shop the same as Google and Facebook. It imposes costs on small businesses that will be much harder for them to bear than it will be for highly profitable companies like Google or Facebook. It seems puzzling that the California legislature actually intended to reach so many businesses that are not in a great position to afford the compliance costs.*<sup>61</sup>

Another troublesome feature the bill shares with GDPR is its “right to erasure.” Although not as far-reaching as the EU’s “right to be forgotten,” the expectation places considerable burden on businesses, which must delete information acquired from that consumer upon request.<sup>62</sup> Businesses are also obligated to provide specific “categories” of various types of information pertaining to individuals, including: (1) “categories of personal information it has collected about that consumer”; (2) “categories of sources from which the personal information is collected”; (3) “business or commercial purpose for collecting or selling personal information”; (4) “categories of third parties with whom the business shares personal information”; and (5) “specific pieces of personal information it has collected about that consumer.”<sup>63</sup>

Businesses are further obligated to allow users to opt-out of information collection “at any time,”<sup>64</sup> and are required to preemptively disclose the intended purpose(s) of the data categories collected from consumers.<sup>65</sup> Prior to that collection, a business must “inform consumers as to the categories of personal information to be

collected and the purposes for which the categories of personal information shall be used.”<sup>66</sup> These rules, as explained later, are likely to significantly hamper the development and application of AI/ML technologies.

One provision CCPA does not share with GDPR, and which stands out as perhaps its most problematic feature is 1798.125(a)(1), which stipulates that “[a] businesses shall not discriminate against a consumer because the consumer exercised any of the consumer’s rights” under CCPA, “including, but not limited to, by:”<sup>67</sup>

- A. “Denying goods or services to the consumer”;
- B. “Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties”;
- C. “Providing a different level or quality of goods or services to the consumer, if the consumer exercises the consumer’s rights under this title”; or
- D. “Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.”<sup>68</sup>

This language creates a very clear free-rider problem. That is, if businesses cannot exclude customers from accessing their products, or provide products at different prices or quality based on an individual’s tolerance for data collection practices, then consumers have little incentive to permit collection. As a result, products and services that were once low- or zero-priced are likely to increase in cost. This is especially true for services like social media, email, and other Internet-based products, but also has the unfortunate effect of artificially inflating the price of developing AI/ML technologies by increasing the cost of accessing new data sets that can be fed into the systems to improve decision-making.

Confusingly, under 1798.125(a)(2), the bill specifically allows for differential pricing “if that difference is reasonably related to the value provided to the consumer by the consumer’s data.”<sup>69</sup> Additional internal contradictions allow businesses to “offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information,”<sup>70</sup> so long as those financial incentives are not “unjust, unreasonable, coercive, or usurious.”<sup>71</sup> What constitutes an “unreasonable” or “usurious” incentive practice, or differential pricing that is “reasonably related to the value” of consumer data, remains anyone’s guess. Indeed, as described previously in Part I, the lack of a clear price on data — and the practical limitations on setting such a price — makes interpreting these exceptions extremely difficult, and its inclusion practically meaningless.

In addition to these specific problems, the central issue with CCPA, is its failure to consider the borderless nature of the Internet. Hahn and Layne-Farrar make this abundantly clear:

*Considering the interstate (and indeed, inter-country) nature of the Internet, state-level legislation seems more likely to obstruct online commerce without providing balanced privacy protection for the nation as a whole. Moreover, [some] argue that states are less likely to employ economic cost-benefit analysis in debating potential bills, and thus may end up causing more consumer harm than they prevent.*<sup>72</sup>

Ultimately, the actual impact of CCPA will be difficult to measure until it goes into effect in 2020. Given the many similarities with GDPR, however, the bill, as currently written, is likely to have similar impacts on California’s digital economy, with unintended and as-yet unforeseeable consequences for the broader American digital ecosystem.

### 3. Self-Regulating Mechanisms

Of course, where existing laws and statutes may fail to address consumer harms, the private sector, despite claims to the contrary, has been a remarkably reliable steward of consumer data and privacy. This is the great unheralded story of the digital advertising and online service platform markets: they are already governed by an effective self-regulatory regime.

Numerous self-regulatory frameworks and third-party certification organizations provide effective governance and oversight of consumers' data. Although a full accounting of these various organizations and consortia is beyond the remit of these comments, two such organizations are worth mentioning: the Network Advertising Initiative (NAI) and the Digital Advertising Alliance (DAA). Both NAI and DAA provide a number of these self-regulatory frameworks, holding participating companies accountable to a complex set of interlocking standards and best practices depending on the industry.<sup>73</sup> Compliance with these principles is reviewed regularly. If consumers experience particular harms as a result of member companies failing to abide by the NAI or DAA guidelines, complaints can be filed directly to the Better Business Bureau through a conveniently-located and prominently-displayed link on the organizations' websites.

In addition to compliance assessments and direct consumer complaints available through organizations like NAI and DAA, many individual firms provide tools directly to users, allowing them to directly control their web browsing experience, and information that online service providers would otherwise have access to. Such tools include:

1. Native browser controls — usually built-in under the browser's "settings" — for controlling Internet-based advertising cookies (on both mobile and desktop versions);<sup>74</sup>
2. Advertising identification controls for mobile devices, which allow users to control access to, and opt-out of, their advertising ID, as well as cross-app advertising (usually found under "Settings"/"Ads" on Android operating systems or "Settings"/"Privacy"/"Advertising" on iOS7 and later); and
3. The AdChoice icon displayed on ads that populate various websites, providing consumers the opportunity to click-through and learn more about the specific types of information used to determine target ads to individuals.

While not perfect solutions to the many complex problems likely to emerge in digital markets, these types of tools, and the self-regulatory regimes that incentivize their propagation, put users in as much (or as little) control of their digital footprint as they desire.<sup>75</sup>

## B. Other Proposed Rules and Regulations

Many of the provisions of both GDPR and CCPA are potentially crippling for future innovative applications of AI/ML. "Purpose specification" rules, such as those mandated under both GDPR and CCPA, would "prohibit the reuse of data for purposes not compatible ... with those for which it was first collected," and have the economically-undesirable effect of preventing companies from experimenting with non-sensitive consumer data for developing new, welfare-enhancing applications.<sup>76</sup> Additionally, forcing anonymization of data, while no doubt an important privacy safeguard in certain contexts, has the unfortunate outcome of limiting the usefulness of various types of information, especially in the context of scientific and medical research.<sup>77</sup>

Another idea that has been incorporated into both GDPR and CCPA is the requirement for firms to obtain affirmative opt-in consent for data collection and/or use. While seemingly a low-cost, high-impact measure for empowering consumers, shifting away from the current arrangement — where consumers must opt-out of data collection practices — has significant economic implications. For example, opt-in requirements have the effect of raising the cost for acquiring the collection and use of data (in the form of permission costs), which is invariably passed on to consumers, either in the form of higher prices or a reduction in quantity, quality, or access to goods and services.<sup>78</sup>

Ultimately, evaluating the differences between opt-in versus opt-out defaults requires, first and foremost, an acceptance that transaction costs not only exist, but can indeed be quite costly. If, for example, online service providers and other Internet-based industries are obligated to provide an affirmative opt-in to data collection and sharing, that can have significant consequences for the health and vibrancy of the online advertising industry. In a 2000 survey analysis, when presented with either a “no-action default” of non-participation (requiring an affirmative opt-in consent for data collection), 48 percent of respondents chose not to permit data collection; by contrast, the “no-action default” of participation rate was fully double — 96 percent.<sup>79</sup> An additional, and important, takeaway from this survey analysis was that the specific framing of the question — whether negative or positive, small or large font, “yes” or “no” answers checked by default etc. — had a significant impact on how participants responded to the prompt.<sup>80</sup> Describing the implications of whether a no-action default ought to fall to opt-in as opposed to opt-out requirements, Hahn and Layne-Farrar accurately diagnose the central concern of the former approach:

*Opt-in can lead to less information sharing not because people who genuinely value privacy are no longer allowing their personal data to be traded, but rather because companies may find it too expensive to administer an opt-in program and because, due to inertia, people simply accept the opt-in no-sharing default regardless of their privacy preferences. An opt-in rule would therefore be inefficient because it could discourage too many individuals from participating.<sup>81</sup>*

These behavioral analyses raise complicated questions regarding the wisdom in shifting towards a default opt-in regime for online data collection. It also raises an important question regarding the extent to which consumer surveys and stated preferences should inform legislation or rulemaking on this debate. In his 2001 testimony, Alan Westin addressed this issue in the context of the opt-in vs opt-out debate:

*It worries me if there would be any kind of legislative standard to opt-in as the requirement or the default because I think that all the survey research shows that consumers want choice, but they don't want somebody to dictate what their choice is. And I think notice and choice, to me, especially in the Internet environment, means stating what the Website wants the information for, how it will use it, and to give the individual a choice then to opt-out or not to do business with the Web site.*

*So, I would argue that all the survey material tells you that the public is seeking tools for confidence. What Congress can do, in my judgment, is to provide a piece of framework legislation that allows then the good businesses to have good relations with the consumers who come to their Web sites, but allows consumers not to do business with those companies that are not posting the kind of privacy policies that the consumer wants to expose themselves to. ...*

*[I]n crafting legislation, putting the choices between, let us say, an opt-in or an opt-out regime into a survey in a way that you give much credence to the response of the individual, it is very difficult because that is a question in which you are really struggling to figure out what the effects would be of one regime in terms of the confidence of consumers to business and the business model, as to how they are going to make money on the Internet.*

*So, what I was trying to suggest is that consumers can express concern, but when legislators go to decide what the way to respond to that concern is, that is where legislative skills and policy analysis and cost-benefit analysis is what you have to bring to bear. I have never seen a good survey on cost-benefit analysis in privacy that I would put much credence in.*<sup>82</sup>

As noted previously in the context of self-regulatory governing bodies, online service providers and advertisers offer an array of tools for not only minimizing consumers' exposure to data collection and tracking, but also opting out of cookies for digital advertising.<sup>83</sup> Additional opt-out tools are also provided through direct browser extensions, such as Chrome<sup>84</sup> and Firefox.<sup>85</sup>

## C. Summary

**Do restrictions on the use of computer and machine learning and data analytics affect innovation or consumer rights and opportunities in existing or future markets, or in the development of new business models?**

While many of these rules and proposals are no doubt offered with the best of intentions, they are more likely to diminish rather than enhance consumer welfare, while similarly forestalling the development and adoption of advancements in AI/ML technologies. Such rules are ultimately doomed to fail consumers for many reasons, but can generally be sorted into two general buckets of criticism.

### 1. The Costs of Omnibus Privacy Regulations

First, in crafting broad, precautionary privacy and data protection rules, there is almost no discernible consideration ever given to the many complicated trade-offs. That is to say, purportedly strengthening data and privacy protection rules comes at a cost to consumer welfare as well as competition and innovation. The following is a partial inventory of the zero-sum trade-offs that are seldom discussed in these debates, but which take some form in either (or both) the GDPR or CCPA rules.

1. A right to be forgotten, by its nature, is in direct conflict with free speech. The more control an individual has over amending (or deleting entirely) his or her past public commentary, the less freely information can flow. Or, put another way, the level of censorship across society rises as each individual's control over information *about* him or her increases.
2. Greater restrictions on data collection and limitations on their use naturally obstructs more sizable gains in AI/ML innovation, through increased development costs and disincentivizing greater levels of investment. In the same way that enhancing individuals' control over their information restricts the free flow of information, so too does restricting the collection of that information inhibit potentially beneficial, and entirely unforeseeable, future applications of that data for AI/ML purposes. The end result is a net decrease in consumer welfare, as consumers lose out on products and services that may otherwise have benefited them.
3. A more extensive and stringent corpus of rules governing how firms can collect, analyze, and retain user data necessitates a greater degree of specialized knowledge in order to ensure legal compliance. Resources devoted to privacy counsels and data protection officers are resources that cannot be apportioned to other, higher-leveraged uses — including investing in AI/ML talent. Higher compliance costs also invariably result in wide-reaching ripple effects that:
  - a. Diminish future innovation and consumer welfare by limiting access to, and use of, data;

- b. Imperil the jobs and livelihoods of the hundreds of thousands of people working in industries tied to the digital economy;
  - c. Provide a structural advantage to incumbent firms (i.e., those with the resources to invest in greater compliance and oversight) over their would-be competitors;<sup>86</sup> and
  - d. Inevitably result in decreased data and privacy protections for users as firms have increased incentives to use the new heightened legal compliance requirements as a liability shield.
4. Self-regulatory governance approaches (e.g., industry standards and best practices, third-party certification and compliance consortia), which provide greater responsiveness and flexibility to changing technological circumstances and consumer expectations, are deprioritized and defunded as firms recalibrate their regulatory strategies to simply absorb the costs of legal compliance. Thus, the result of statutorily-defined rules replacing more adaptive regulatory governance mechanisms better suited to the dynamism of digital markets is a more sclerotic, less consumer-friendly market — that is, an environment in which total consumer welfare is reduced.

The second, more fundamental problem with comprehensive privacy regulations is that they offer a solution before ever identifying a “problem” to be solved. As discussed previously, consumer expectations of privacy cannot be condensed to a simple framework of “more is better.” Yet that is precisely how many advocates and regulators frame the issue: presuming to know consumers care about privacy at the expense of all other competing values without any empirics to substantiate the claim. As a result, the provisions that end up being inserted into sweeping privacy edicts are usually characterized by vague, disjointed, and occasionally contradictory language.<sup>87</sup> This is a classic case study in how *not* to regulate a perceived market failure. By asserting a problem exists without substantiating the underlying claim (e.g., privacy is important and people don’t have “enough” of it), the proposed remedy (e.g., minimize the amount of data collected) will seldom take account of the full scope of costs and benefits, which fundamentally constrains the possibility of considering alternative regulatory corrective measures.

In short, the problem with this approach to governing privacy and consumer data is that the rules assume (1) privacy is not subject to zero-sum cost trade-offs, and (2) presumes to offer a solution before identifying a problem to be solved.

There is a high likelihood rules that raise the costs of various data collection practices will create an ecosystem of “anticompetitive lock-in,” in which established firms, already equipped with the resources necessary to meet higher compliance burdens, will crowd out new market entrants. This effect could be particularly acute not only for the largest online service platforms, such as Facebook and Google, but also for the digital advertising market. In a recent white paper from Columbia University’s Tow Center for Digital Journalism, Susan McGregor and Hugo Zylberberg articulate this concern, and the breadth of provisions that may contribute to innovation sclerosis in digital markets:

*As of 2017, Google and Facebook claim seventy-seven cents of every dollar spent on digital advertising in the United States, with no other single company claiming even as much as three percent of the total market share. While the GDPR may hinder some of these companies’ data collection and/or sharing activities, the regulation may well squeeze smaller advertising networks even more, potentially magnifying the dominance of this duopoly in online advertising. These smaller ad networks, for example, typically lack the direct consumer relationships needed to secure consent from users on their own behalf, but may also find that media publishers and other website hosts are reluctant to ask for user consent for the broad range and volume of data that these advertisers can presently access without hindrance. Without access to the data on which they currently rely, smaller advertising*

*networks may be simply cut out of the online market altogether unless they can find a way to gain some advantage over the platforms in compliance, user-friendliness, or rates. In this environment, platform companies and website hosts—such as media companies—that have a brand-name relationship to their users are likely to have more success in persuading individuals to give up their information, and therefore may have increased power in the advertising market under the GDPR.<sup>88</sup>*

Although McGregor and Zylberberg ultimately conclude that “the net effect of [GDPR] may well be positive in the long term,” they correctly recognize the potential costs to competition that rules restricting data collection could present.<sup>89</sup> For new firms looking to utilize data-intensive AI/ML technologies, such rules will present considerable barriers to entry.<sup>90</sup>

Similarly problematic are the provisions in both bills that provide consumers with new de facto ownership rights over the data they generate in online activities. While that may seem like an ideal remedy to the purported problems that plague digital markets, it fails to account for the investments that firms make in collecting and manipulating those bits of information. The data exhaust that consumers produce in their online interactions and engagements is not, by itself, fundamentally valuable; the economic value of such information is created by businesses, researchers, and other actors generating new insights and data from the information that consumers essentially leave behind. The use of such data in AI/ML improvements is one such example.<sup>91</sup>

Strict, one-size-fits-all data protection and privacy regulations are fundamentally anti-consumer and anti-innovation — anti-consumer because they drive up costs and diminish competition, and anti-innovation because they stifle the development of new products and services while incentivizing firms to prioritize regulatory compliance over maximizing consumer welfare.<sup>92</sup> Additionally, by assuming the existence of a problem requiring a solution, such rules fail to adequately assess the costs and benefits of alternative governance strategies. Finally, when compared to a light-touch, sector-based regulatory approach to addressing privacy harms, it’s not at all clear that broad data protection mandates would do a better job of promoting consumer privacy interests, and may actually have the opposite effect.

The problem with omnibus privacy regulations is that they disregard the difficulty inherent in governing “large, diverse, and complex economic ecosystems,” and “will inevitably result in unintended (though often foreseeable) consequences – not only for firms and economic agents but also for free speech and expression. While they may be crafted with the best of intentions, far-reaching rules and regulations fail to account for the inherent dynamism of market economies, and such rules can never fully or accurately account for the future opportunities and challenges that will arise.”<sup>93</sup>

As regulators consider new rules governing AI/ML, the European approach should serve as a cautionary tale. The FTC should take heed of the unfolding crisis in EU digital markets, and recognize rules such as GDPR for what they are: vague and prescriptive policy kludges that act as an innovation repellent, threatening high fines and broad-discretionary enforcement actions unmoored from evidentiary analysis.

## **2. Algorithmic Accountability: An Alternative Regulatory Framework for AI**

In a recent report for the Brookings Institution, Cameron Kerry, the former Acting Secretary and General Counsel of the Department of Commerce, noted the benefits of many GDPR provisions, but ultimately concluded that the law “takes a much more prescriptive and process-oriented approach” than would be desirable.<sup>94</sup> In particular, he reasoned that whatever its virtues, GDPR “may not prove adaptable to [AI] and new technologies like autonomous vehicles that need to aggregate masses of data for [ML] and smart infrastructure.”<sup>95</sup> He continues:

*Strict limits on the purposes of data use and retention may inhibit analytical leaps and beneficial new uses of information. A rule requiring human explanation of significant algorithmic decisions will shed light on algorithms and help prevent unfair discrimination but also may curb development of [AI].<sup>96</sup>*

While making AI systems “explainable” would certainly help consumers, so would explainability in all decisions to which consumers are subject. As Joshua New and Daniel Castro of the Center for Data Innovation note in a recent report on the this topic, rules that mandate algorithmic transparency and explainability “hold algorithmic decisions to a standard that simply does not exist for human decisions,” and fail to recognize how “algorithms are simply a recipe for decision-making.”<sup>97</sup> They go on:

*If proponents of algorithmic transparency and explainability are concerned that these decisions are harmful, then it is counterproductive to only call for algorithmic decisions to be transparent or explainable, rather than for all aspects of all decision-making to be made public or explained. If blanket mandates for transparency and explainability are appropriate for algorithmic decision-making, but not human decision-making (which itself is often supported by computers), logic would dictate that human decisions are already transparent, fair, and free from unconscious and overt biases. In reality, bias permeates every aspect of human decision-making, so to hold algorithms to a higher standard than for humans is simply unreasonable.<sup>98</sup>*

As such, mandating explainability or total transparency in AI/ML would fail to provide any reasonable, actionable insights for consumers. The simple reality is that there is nothing to be gleaned from these levels of transparency, especially in ML systems that rely on thousands of layers of simulated neurons to interpret data inputs.<sup>99</sup>

Nor would it be desirable to promote rules that mandate complete transparency, requiring AI/ML source code to be made publicly available for review. As a recent Harvard Business Review article aptly noted, the “black box” of AI isn’t necessarily an impediment to promoting user trust. It is true that “users will not trust black box models, but they don’t need – or even want – extremely high levels of transparency. That means responsible companies need not fret over what percentage of source code to reveal, or how to help users ‘read’ massive datasets. Instead, they should work to provide basic insights on the factors driving algorithmic decisions.”<sup>100</sup> As researchers work to develop technologies capable of providing that level of basic explainability, the FTC and regulators should prioritize a framework of flexible, adaptive standards that hold the operators, not developers, of AI/ML systems accountable for the use of algorithms. Such a framework of “algorithmic accountability,” as specifically detailed by New and Castro, would apply existing laws to algorithmic decisions while embracing industry self-regulation in those contexts where it suffices “an adequate means of governance.”<sup>101</sup>

Rather than endorsing rules that set unreasonable expectations of explainability and transparency — expectations that even human decision-making is not held to — the FTC should embrace mechanisms that prioritize holding firms accountable for the *outcomes* of algorithmic decisions. Such an approach would marry the current sector-based privacy landscape of privacy rules, with a set of technologically-neutral, evidence-based standards for determining the existence of, and remedy for, a particular consumer harm.

## **PART III: SUMMARY OF RECOMMENDATIONS**

The implications of AI/ML are potentially profound — not only for economic growth and increases in consumer welfare, but for the welfare of society more generally. Whether in the realm of healthcare research, government accountability and oversight, or commercial applications more generally, this technology holds promising potential and should not be unnecessarily crippled by overzealous rules that promise unworkable

solutions to hypothetical problems. While there may be concerns with the use of AI/ML in particular contexts, existing rules and regulations are more than adequate to remedy those problems as they emerge.

In order to maximize these benefits, while minimizing the potential costs to consumers, the FTC should consider the following recommendations in advance of its Hearings on Competition and Consumer Protection in the 21st Century.

## Consumer Welfare & Privacy Effects of Integrating AI into Digital Markets

1. The FTC should avoid attempting to address the issue of pricing or quantifying the value of data, and, by extension, refrain from considering claims of “data price gouging” as constituting anticompetitive practices; and
2. Consider how recent advancements in AI/ML have helped contribute to better understanding the return on investment for digital advertising and investment, and the implications for assessing gains to consumer welfare.

## How AI Regulations Impact Innovation & Consumer Welfare

1. The FTC should recognize a framework for “algorithmic accountability” as the ideal approach to regulating AI/ML, while promoting self-regulatory governance mechanisms in lieu of broader omnibus privacy rules;
2. Examine how implementing specific rules for “algorithmic accountability” could address potential harms in sector-specific contexts; and
3. When considering “purposes specification” rules for data, data retention mandates, or default opt-in requirements, the FTC should give considerable weight to evidence detailing the economic costs associated with such proposals.

## CONCLUSION

Between 2013 and 2016, venture capital and angel investments in new AI/ML technologies returned annual compound growth rates of 40 percent, compared to 30 percent in the preceding three year period.<sup>102</sup> That growth was only possible because domestic regulators and policymakers abstained from embracing many of the more stridently anti-innovation rules offered by Privacy Fundamentalists.

In order to remain the world leader in innovation and technological progress, the United States should maintain its commitment to the value of existing consumer protection policy tools, sector-specific and technologically-neutral privacy rules, and an ecosystem of light-touch self-regulatory frameworks that provides industry and innovators with the flexibility to continue doing what they do best: making America the envy of the world’s technology markets.

We would like to thank the FTC for the opportunity to comment on these issues and look forward to continued engagement on this and other topics.

---

<sup>1</sup> Statement of Alan F. Westin, Hearing before the Subcommittee on Commerce, Trade and Consumer Protection of the Committee on Energy and Commerce, House of Representatives, “Opinion Surveys: What Consumers Have to Say About Information Privacy,” 107th Congress, 8 May 2001, <https://www.gpo.gov/fdsys/pkg/CHRG-107hhrg72825/html/CHRG-107hhrg72825.htm>.

<sup>2</sup> *Id.*

<sup>3</sup> Adam Satariano, “G.D.P.R., a New Privacy Law, Makes Europe World’s Leading Tech Watchdog,” *The New York Times*, 24 May 2018, <https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html> (“The new privacy rules are part of a ‘strong European tradition’ of policing industries to protect the environment or public health, even if it does ‘constrain business,’ said Margrethe Vestager, Europe’s top antitrust official.”); Emily Stewart, “Why you’re getting so many emails about privacy policies,” *Vox*, 24 May 2018, <https://www.vox.com/policy-and-politics/2018/4/5/17199754/what-is-gdpr-europe-data-privacy-facebook> (“The European sense of privacy as a fundamental human right has been codified in law for a long time,” Michelle De Mooy, the director for privacy and data at the Center for Democracy & Technology. “They have this people-first mentality more than we do here in our capitalist society, where innovation is sort of equated with letting businesses do whatever they need to grow. That has translated into pretty weak data protection.”)

<sup>4</sup> “Privacy Fundamentalists” are those who reject “consumer-benefit or societal-protection claims for data uses” and embrace more stringent “legal-regulatory privacy measures.” See Alan F. Westin, “Social and Political Dimensions of Privacy,” *Journal of Social Issues*, Vol. 59, No. 2, 2003, p. 22, <http://www.privacysummersymposium.com/reading/westin.pdf>.

<sup>5</sup> For a more robust account of these organizations and the various incentives that drive issue prioritization for many, but by no means all, privacy advocates, see Daniel Castro and Alan McQuinn, *The Privacy Panic Cycle: A Guide to Public Fears About New Technologies*, Information Technology and Innovation Foundation (Washington, D.C.: Sep. 2015), p. 9-10, <http://www2.itif.org/2015-privacy-panic.pdf>.

<sup>6</sup> Eli M. Noam, “Privacy and Self-Regulation: Markets for Electronic Privacy,” in *Privacy and Self-Regulation in the Information Age*, U.S. Department of Commerce, 1997, <https://www.ntia.doc.gov/page/chapter-1-theory-markets-and-privacy>.

<sup>7</sup> Alessandro Acquisti, et. al., “The Economics of Privacy,” *Journal of Economic Literature*, Vol. 52, No. 2, 8 March 2016, p. 48, <https://dx.doi.org/10.2139/ssrn.2580411>.

<sup>8</sup> *Attitudes on Data Protection and Electronic Identity in the European Union*, Special Eurobarometer 359, Conducted by TNS Opinion & Social at the request of Directorate-General Justice, Information Society & Media and Joint Research Centre, June 2011, <https://studylib.net/doc/13189647/special-eurobarometer-359-report--attitudes-on-data-prote...>

<sup>9</sup> *Id.* (“They are the most likely to agree that disclosing personal information is not a big issue for them, that they do not mind disclosing personal information in return for free services online, such as a free email address, and that they feel obliged to disclose personal information on the Internet. They are also the most likely to disclose various types of personal information on social networking sites; to disclose personal information on social networking sites ‘for fun’; to usually not read privacy statements on the Internet, but to feel sufficiently informed about the conditions for data collection and the further uses of their data when joining a social networking site or registering for a service online; to trust all authorities, institutions and commercial companies; to have changed their personal profile from the default settings on a social networking site or sharing site; and to hold the social networking or sharing sites responsible for safe handling of data.”)

<sup>10</sup> See Alessandro Acquisti, et. al., “What Is Privacy Worth?,” *Journal of Legal Studies*, Vol. 42, June 2013, [https://www.hbs.edu/faculty/Publication%20Files/AcquistiJohnLoewenstein13\\_334936de-38a8-4d99-b90c-c3c02dae48b2.pdf](https://www.hbs.edu/faculty/Publication%20Files/AcquistiJohnLoewenstein13_334936de-38a8-4d99-b90c-c3c02dae48b2.pdf).

<sup>11</sup> Bernardo A. Huberman, et. al., *Valuating Privacy*, IEEE Security & Privacy, 2005, <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.71.1089&rep=rep1&type=pdf>. (“Our hypothesis - and the motivation for our study - is that people reveal information when they feel that they’re somewhat typical or positively atypical compared to the target group. To test this hypothesis, we conducted experiments that elicit the value people place on their private data. We found, with great significance (more than 95 percent statistical confidence) that a linear relationship exists between an individual’s belief about a trait and the value he or she places on it. That is, the less desirable the trait, the greater the price a person demands for releasing the information.”)

<sup>12</sup> See Alastair Beresford, et. al., *Unwillingness to Pay for Privacy: A Field Experiment*, IZA Discussion Paper No. 5017, 6 July 2010, [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1634484](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1634484); see also Jens Grossklags and Alessandro Acquisti, *When 25 Cents is too much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information*, Workshop on the Economics of Information Security, 7 June 2007, [http://people.ischool.berkeley.edu/~jensg/research/paper/Grossklags\\_Acquisti-WEISo7.pdf](http://people.ischool.berkeley.edu/~jensg/research/paper/Grossklags_Acquisti-WEISo7.pdf).

<sup>13</sup> *Consumers driving the digital uptake: The economic value of online advertising-based services for consumers*, McKinsey & Company, September 2010, p. 5, [http://www.youronlinechoices.com/white\\_paper\\_consumers\\_driving\\_the\\_digital\\_uptake.pdf](http://www.youronlinechoices.com/white_paper_consumers_driving_the_digital_uptake.pdf).

<sup>14</sup> *Id.*, p. 6.

<sup>15</sup> *Id.*

<sup>16</sup> Austan Goolsbee and Peter J. Klenow, *Valuing Consumer Products by the Time Spent Using Them: An Application to the Internet*, NBER Working Paper No. 11995, Jan. 2006, <http://www.nber.org/papers/w11995.pdf>.

<sup>17</sup> Robert W. Hahn and Anne Layne-Farrar, *The Benefits and Costs of Online Privacy Legislation*, AEI-Brookings Joint Center for Regulatory Studies, Working Paper 01-14 (Washington, D.C.: Oct. 2001), p. 18, [http://papers.ssrn.com/abstract\\_id=292649](http://papers.ssrn.com/abstract_id=292649). (“Consumers may initially find it difficult to determine a reasonable price for their information. Commercial buyers will have a much better notion of the value of a particular piece of personal information — individuals may not get “market value” in this case. A related problem is that an individual’s information may not have genuine commercial value per se; that is, information may be valuable only if it is combined with other information for that individual or is available for some threshold number of individuals. As a result, under some circumstances Web sites could have a bargaining advantage over individuals.”)

<sup>18</sup> Ryan Hagemann, *Data Price Gouging: A Stalking Horse for a Neo-Brandeisian Antitrust Doctrine?*, Niskanen Center (Washington, D.C.: 8 May 2018), [https://niskanencenter.org/wp-content/uploads/2018/05/Brief-Data-Price-Gouging-A-Stalking-Horse-for-a-Neo-Brandeisian-Antitrust-Doctrine\\_.pdf](https://niskanencenter.org/wp-content/uploads/2018/05/Brief-Data-Price-Gouging-A-Stalking-Horse-for-a-Neo-Brandeisian-Antitrust-Doctrine_.pdf).

<sup>19</sup> Joaquin Quiñonero Candela, et. al., “Counterfactual Reasoning and Learning Systems: The Example of Computational Advertising,” *Journal of Machine Learning Research*, Vol. 14, 3207-3260, p. 3207, 2013.

<sup>20</sup> *Id.*, p. 3209.

<sup>21</sup> For a more detailed examination of consumer benefits and harms in online markets in the wake of the recent Supreme Court decision in *Ohio v. American Express Co.*, see Alec Stapp, *Reports of Antitrust’s Death Have Been Greatly Exaggerated: Economics, Law, and Technology in the Supreme Court’s Amex Decision*, Niskanen Center (Washington, D.C.: July 2018), <https://niskanencenter.org/wp-content/uploads/2018/07/Reports-of-Antitrusts-Death-Have-Been-Greatly-Exaggerated.pdf>.

<sup>22</sup> Alex Porter, “The Impact of Artificial Intelligence on the Future of the Digital Agency,” *Forbes*, 8 May 2018, <https://www.forbes.com/sites/forbesagencycouncil/2018/05/08/the-impact-of-artificial-intelligence-on-the-future-of-the-digital-agency/#1bb719327d63>. (“[T]he real value in AI is its ability to analyze that data and endorse strategic action ... delivering personalized content at scale based on collected data and analysis. ... [M]any agencies have already been using AI and machine learning to optimize ads and personalize the customer experience — with positive results. This experience allows those at the forefront to quickly adapt to the effects of AI on their industry.”)

<sup>23</sup> Sami Main, “Programmatic Digital Display Ads Now Account for Nearly 80% of US Display Spending,” *AdWeek*, 18 Apr. 2017, <https://www.adweek.com/tv-video/programmatic-digital-display-ads-now-account-for-nearly-80-of-us-display-spending/>.

<sup>24</sup> *What is an untrustworthy supply chain costing the US digital advertising Industry?*, IAB US Benchmarking Study, Nov. 2015, pp. 27-36, [https://www.iab.com/wp-content/uploads/2015/11/IAB\\_EY\\_Report.pdf](https://www.iab.com/wp-content/uploads/2015/11/IAB_EY_Report.pdf).

<sup>25</sup> *Id.*

<sup>26</sup> *Ad Fraud to Cost Advertisers \$19 Billion in 2018, Representing 9% of Total Digital Advertising Spend*, Juniper Research Press Release, 26 Sep. 2017, [https://www.juniperresearch.com/press/press-releases/ad-fraud-to-cost-advertisers-\\$19-billion-in-2018](https://www.juniperresearch.com/press/press-releases/ad-fraud-to-cost-advertisers-$19-billion-in-2018).

<sup>27</sup> “How We Prevent Click Fraud,” PPC Protect, <https://ppcprotect.com/how-it-works/>.

<sup>28</sup> “NOIZ is an AI-enabled, decentralized cognitive advertising network that uses blockchain” to combat ad fraud. *AI + Blockchain + Social Impact: an advertising trifecta*, NOIZ white paper discussion draft, <https://drive.google.com/file/d/1dIZPn7-AIO6LiltrmYKcNDPzeNZt9vpK/view>.

<sup>29</sup> See Mary Meeker, *Internet Trends Report 2018*, 30 May 2018, <https://www.kleinerperkins.com/perspectives/internet-trends-report-2018>. The top technology firms in the United States (Apple, Amazon, Google, Microsoft, Facebook, Intel, Cisco, Oracle, IBM, NVIDIA, Adobe, Texas Instruments, Salesforce, Qualcomm, Micron Technologies) account for almost \$5 trillion in total market capitalization; the Asia Pacific region's top technology firms (Tencent, Samsung, Taiwan Semiconductor, Broadcom, Container Store, Sony, Nintendo) account for almost \$1.4 trillion; the top European technology firms (SAP, Accenture, ASML Holding) together account for a mere \$285 billion in total market capitalization.

<sup>30</sup> Federico Biagi, *ICT and Productivity: A Review of the Literature*, Joint Research Centre of the European Commission Technical Report, Institute for Prospective Technological Studies, Digital Economy Working Paper 2013/09, <http://ftp.jrc.es/EURdoc/JRC84470.pdf>.

<sup>31</sup> This refers to the point at which a VC sells its stake in a firm to realize gains (or losses) – generally planned during the initial investment phase(s) and predicated on a predetermined set of threshold criteria.

<sup>32</sup> Jacques Bughin, et. al., *Artificial Intelligence: The Next Digital Frontier?*, McKinsey Global Institute, Discussion Paper, June 2017, p. 18, <https://www.mckinsey.com/-/media/mckinsey/industries/advanced%20electronics/our%20insights/how%20artificial%20intelligence%20can%20deliver%20real%20value%20to%20companies/mgi-artificial-intelligence-discussion-paper.ashx>.

<sup>33</sup> Federal laws governing privacy include, among others, the Cable Communications Policy Act of 1984, CAN-SPAM Act of 2003, Children's Online Privacy Protection Act, Do-Not-Call Implementation Act of 2003, Driver's Privacy Protection Act, Electronic Communications Privacy Act, Family Educational Rights and Privacy Act, Genetic Information Nondiscrimination Act, Gramm–Leach–Bliley Act, Health Insurance Portability and Accountability Act, Omnibus Crime Control and Safe Streets Act of 1968, Privacy Act of 1974, Right to Financial Privacy Act, Telephone Consumer Protection Act of 1991, Telephone Records and Privacy Protection Act of 2006, and Video Privacy Protection Act.

<sup>34</sup> Hahn and Layne-Farrar, *supra* note 17 at 43.

<sup>35</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, Article 13(1)(c), [hereafter, "GDPR"].

<sup>36</sup> GDPR, Article 14.

<sup>37</sup> GDPR, Article 15(1).

<sup>38</sup> GDPR, Article 17(1).

<sup>39</sup> GDPR, Article 22. (Individuals are “not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her, or similarly significantly affects him or her.”)

<sup>40</sup> *Id.* (In order “to qualify as human intervention, the controller must ensure that any oversight of the decision is meaningful, rather than just a token gesture. It should be carried out by someone who has the authority and competence to change the decision,” and requires the analyst to “consider all the relevant data” implicated by the outcome of an algorithmic decision.)

<sup>41</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, Recitals, <https://gdpr-info.eu/recitals/>.

<sup>42</sup> Nick Wallace and Daniel Castro, *The Impact of the EU's New Data Protection Regulation on AI*, Center for Data Innovation (Washington, D.C.: March 2018), pp. 9-10, <http://www2.datainnovation.org/2018-impact-gdpr-ai.pdf>.

<sup>43</sup> *Id.*, pp. 15-17.

<sup>44</sup> See Nick Wallace, “Overzealous EU Data Protection Regulations Are More Likely to Take Your Job Than a Robot,” *City A.M.*, 2 Mar. 2017, <http://www.cityam.com/260087/overzealous-eu-data-protection-regulations-more-likely-take>. (“[T]he truth is American tech giants are already better equipped than most to fill these positions, so the GDPR will actually tip the competitive balance further in their favour. Smaller foreign firms are likely to shun Europe and focus their comparatively limited resources on more accessible markets, while European startups will find it costlier to get off the ground in the first place. These problems come alongside many other costs and limitations imposed by the GDPR, which will limit European attempts to benefit from data innovation.”); see also Daniel Castro and Michael McLaughlin, “Why the GDPR Will Make Your Online Experience Worse,” *Fortune*, 23 May 2018, <http://fortune.com/2018/05/23/gdpr->

---

[compliant-privacy-facebook-google-analytics-policy-deadline/](#). (“The regulation places significant burdens on organizations. To comply with the GDPR’s requirements, organizations have to buy and modify technology, create new data handling policies, and hire additional employees. For Fortune Global 500 companies, the biggest firms worldwide by revenue, the costs of compliance will amount to \$7.8 billion. In the U.S., PwC surveyed 200 companies with more than 500 employees and found that 68% planned on spending between \$1 and \$10 million to meet the regulation’s requirements. Another 9% planned to spend more than \$10 million. With over 19,000 U.S. firms of this size, total GDPR compliance costs for this group could reach \$150 billion. And this does not include smaller firms and nonprofit organizations, most of which, if they have European customers, will have their own compliance costs.”)

<sup>45</sup> Peter P. Swire and Robert E. Litan, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive*, (Washington, D.C.: Brookings Institution Press, 1998), p. 151 ISBN 0-8157-8240-3.

<sup>46</sup> *Id.*, 157-167.

<sup>47</sup> For example, the Directive’s effects were also felt in the finance industry, where stringent privacy rules resulted in a market in which “financial services [were] provided by far fewer institutions — *one tenth* the number serving U.S. customers, despite the fact that the pan-European market has almost one and one-half times as many households.” Walter Kitchenman, *U.S. Credit Reporting: Perceived Benefits Outweigh Privacy Concerns*, The Tower Group (Jan. 1999).

<sup>48</sup> There is scant evidence to suggest such rules would actually improve user privacy. Rather, the push for such regulation seems predicated more on a *desire* for something to be done, regardless of the impact on the digital economy.

<sup>49</sup> Daniel Lyons, “GDPR: Privacy as Europe’s tariff by other means?,” American Enterprise Institute, 3 July 2018, <https://www.aei.org/publication/gdpr-privacy-as-europes-tariff-by-other-means/>. (“The chilling effect on digital products available to European consumers could be significant. Even if companies are not actively marketing to European residents, they may have European visitors interacting with their webpage, taking advantage of marketing offers, or subscribing to newsletters. If these interactions result in retention of personally identifiable information, the company is subject to the GDPR. The ease with which a company may find itself bound, coupled with the cost of compliance and potentially draconian penalties for violation, creates strong incentives for companies to withdraw — aggressively — from European markets.”)

<sup>50</sup> For example, both Parity ICO Passport Services, which offered identity verification services for owners of Ethereum wallets who have successfully passed ID background checks, and Klout, a social media platform that offered “influence scores” to assess expertise and credibility based on an individual’s relationship network and prior social media posts, both shut down in the weeks prior to GDPR’s date of implementation.

<sup>51</sup> Jessica Davies, “GDPR mayhem: Programmatic ad buying plummets in Europe,” *Digiday*, 25 May 2018, <https://digiday.com/media/gdpr-mayhem-programmatic-ad-buying-plummets-europe/>.

<sup>52</sup> Matthia Bauer, et. al., *The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce*, European Centre for International Political Economy, report commissioned by the U.S. Chamber of Commerce, Mar. 2013, p. 3,

[https://www.uschamber.com/sites/default/files/documents/files/020508\\_EconomicImportance\\_Final\\_Revised\\_lr.pdf](https://www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf). (“If services trade and cross-border data flows are seriously disrupted (assuming that binding corporate rules, model contract clauses and EU-U.S. Safe Harbor framework are no longer recognized), the negative impact on EU GDP could reach -0.8% to -1.3%. EU services exports to the United States drop by -6.7% due to loss of competitiveness. As goods exports are highly dependent on efficient provision of services (up to 30% of manufacturing input values come from services), EU manufacturing exports to the United States could decrease by up to -11%, depending on the industry. In such case, the export benefits produced by the EU-U.S. FTA are eradicated by a good margin.”)

<sup>53</sup> *Id.* (“The direct negative welfare effect (under the same assumptions) of the regulation could reach up to 1,353 USD (1041 euro) per year for a household of four people.”)

<sup>54</sup> *Id.*, p. 21.

<sup>55</sup> Alec Stapp and Ryan Hagemann, “EU Tech Regulation Is the Real Trade War,” *National Review*, 25 July 2018, <https://www.nationalreview.com/2018/07/european-union-tech-regulation-real-trade-war/>.

<sup>56</sup> California Consumer Privacy Act of 2018, § 1798.140(o).

<sup>57</sup> *Id.*, § 1798.140(h).

<sup>58</sup> *Id.*, § 1798.140(a).

---

<sup>59</sup> Eric Goldman, “A First (But Very Incomplete) Crack at Inventorying the California Consumer Privacy Act’s Problems,” Technology and Marketing Law Blog, 24 July 2018, <https://blog.ericgoldman.org/archives/2018/07/a-first-but-very-incomplete-crack-at-inventorying-the-california-consumer-privacy-acts-problems.htm>.

<sup>60</sup> Joseph Jerome and Michelle De Mooy, “A New Day for Privacy Dawns in California,” Center for Democracy and Technology, 3 July 2018, <https://cdt.org/blog/a-new-day-for-privacy-dawns-in-california/>.

<sup>61</sup> Eric Goldman, *An Introduction to the California Consumer Privacy Act (CCPA)*, 31 July 2018, p. 2, [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3211013](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3211013).

<sup>62</sup> California Consumer Privacy Act of 2018, § 1798.105(a), (c). (“A business that receives a verifiable request from a consumer to delete the consumer’s personal information pursuant to subdivision (a) of this section shall delete the consumer’s personal information from its records and direct any service providers to delete the consumer’s personal information from their records.”)

<sup>63</sup> *Id.*, § 1798.110(c).

<sup>64</sup> *Id.*, § 1798.120(a). (“A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer’s personal information.”)

<sup>65</sup> *Id.*, § 1798.100(b).

<sup>66</sup> *Id.*

<sup>67</sup> *Id.*, § 1798.125(a)(1).

<sup>68</sup> *Id.*

<sup>69</sup> *Id.*, § 1798.125(a)(2). (“Nothing in this subdivision prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the consumer by the consumer’s data.”)

<sup>70</sup> *Id.*, § 1798.125(b)(1)

<sup>71</sup> *Id.*, § 1798.125(b)(4).

<sup>72</sup> Hahn and Layne-Farrar, *supra* note 17 at 43.

<sup>73</sup> A more robust accounting of these frameworks, best practices, and standards can be found at:

<https://youradchoices.com/principles>

<sup>74</sup> As a small set of examples, see the following: Chrome:

<http://support.google.com/chrome/bin/answer.py?hl=en&answer=95647> (desktop),

<https://support.google.com/chrome/answer/2392709?hl=en> (mobile); Safari: <http://support.apple.com/kb/PH11913>

(desktop), <https://support.apple.com/en-us/HT201265> (mobile); Firefox: [http://support.mozilla.org/en-](http://support.mozilla.org/en-US/kb/Enabling%20and%20disabling%20cookies#w_how-do-i-change-cookie-settings)

[US/kb/Enabling%20and%20disabling%20cookies#w\\_how-do-i-change-cookie-settings](http://support.mozilla.org/en-US/kb/Enabling%20and%20disabling%20cookies#w_how-do-i-change-cookie-settings) (desktop),

<https://support.mozilla.org/en-US/kb/clear-your-browsing-history-and-other-personal-dat> (mobile);

<sup>75</sup> These self-regulatory frameworks are also an example of “soft law,” described as “instruments or arrangements that create substantive expectations that are not directly enforceable, unlike ‘hard law’ requirements such as treaties and statutes.” See Ryan Hagemann, et. al., “Soft Law for Hard Problem: The Governance of Emerging Technologies in an Uncertain Future,” *Colorado Technology Law Journal*, (forthcoming),

[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3118539](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3118539); see also Ryan Hagemann “New Rules for New Frontiers: Regulating Emerging Technologies in an Era of Soft Law,” *Washburn Law Journal*, Vol. 57, No. 2, 235-263 (Spring 2018), <http://contentdm.washburnlaw.edu/cdm/ref/collection/wlj/id/6797>.

<sup>76</sup> Alan McQuinn and Daniel Castro, *Why Stronger Privacy Regulations Do Not Spur Increased Internet Use*, Information Technology and Innovation Foundation (Washington, D.C.: July 2018), p. 22, <http://www2.itif.org/2018-trust-privacy.pdf>.

<sup>77</sup> *Id.*, p. 18. (“Even where compelling commercial use cases have been engineered and are demanded by firms, regulatory and social barriers can raise the cost and slow the rate of adoption. Product liability is one such concern; it is especially troublesome for automakers and other manufacturers. Privacy considerations restrict access to data and often require it to be anonymized before it can be used in research.”)

<sup>78</sup> Hahn and Layne-Farrar, *supra* note 17 at 58. (“Opt-in can lead to less information sharing not because people who genuinely value privacy are no longer allowing their personal data to be traded, but rather because companies may find it too expensive to administer an opt-in program and because, due to inertia, people simply accept the opt-in no-

---

sharing default regardless of their privacy preferences. An opt-in rule would therefore be inefficient because it could discourage too many individuals from participating.”)

<sup>79</sup> Steven Bellman, et. al., “To Opt-In Or To Opt-Out? It Depends On The Question,” *Communications of the ACM*, 13 Nov. 2000.

<sup>80</sup> *Id.*

<sup>81</sup> Hahn and Layne-Farrar, *supra* note 17 at 58.

<sup>82</sup> Statement of Alan F. Westin, *supra* note 1.

<sup>83</sup> These tools are provided by a number of industry associations previously mentioned, including NAI, DAA, and AppChoices. See generally <https://www.networkadvertising.org/choices>, <http://www.aboutads.info/choices/>, and <http://www.aboutads.info/appchoices>.

<sup>84</sup> See generally Chrome Web Store, <https://chrome.google.com/webstore/search/extensions/cookies%20privacy>.

<sup>85</sup> See generally Firefox Add-ons, Privacy & Security, <https://addons.mozilla.org/en-US/firefox/extensions/privacy-security/>.

<sup>86</sup> This is an issue that merits special attention for the FTC, and which will be discussed in greater length in the summary for Part III.

<sup>87</sup> This should come as no surprise, of course; building a codified set of privacy rights atop our conventional expectations of privacy is a naturally problematic undertaking, as those expectations are based in no small part on technology and how each individual weighs the costs and benefits of technological adoption at any given moment. See Ryan Hagemann, “How We Think About Privacy Matters,” Niskanen Center (Washington, D.C.: 16 June 2016), <https://niskanencenter.org/blog/think-privacy-matters/>. (“The trouble with building an idea of privacy rights atop conventional expectations of privacy is that our expectations are based to a significant extent on technology. But today’s most pressing controversies about privacy arise precisely because technology has advanced so fast and our conventional expectations haven’t caught up. The way those conventions shake out will depend to a large extent on the rules we do or don’t put in place to regulate access to personal information. The use of new technologies may violate current privacy conventions while also promising to deliver momentous benefits. For example, delivery drones will, as a matter of course, be able to see activity on private property that otherwise would have been entirely invisible. But it’s crucial to recognize the possibility that our interests in enjoying the benefits of delivery drones may ultimately outweigh our interests in, say, not being caught on camera sunbathing in the buff. If privacy expectations built around older technologies are allowed to rule, we may lose out on the benefits of innovation.”)

<sup>88</sup> Susan E. McGregor and Hugo Zylberberg, *Understanding the General Data Protection Regulation: A Primer for Global Publishers*, Tow Center for Digital Journalism at Columbia University (New York, NY: Mar. 2018), pp. 37-38, <https://doi.org/10.7916/D8K08GVB>.

<sup>89</sup> *Id.*, p. 56.

<sup>90</sup> See Sean Heather, Comments to the National Telecommunications and Information Administration, Subject; International Internet Policy Priorities, Chamber of Commerce, 17 July 2018, p. 9. (“[M]ost small businesses and startups already start at a disadvantage against larger, existing players that have massive amounts of data to utilize. Having to comply with GDPR creates further disadvantages for small businesses as they are unable to access complex legal and compliance guidance easily.”)

<sup>91</sup> Lucas Bergkamp, “EU Data Protection Policy: The Privacy Fallacy: Adverse Effects of Europe’s Data Protection Policy in an Information-Driven Economy,” *Computer Law & Security Report*, Vol. 18, No. 1 (Brussels, Belgium: 2002), p. 39, [https://www.huntonak.com/files/Publication/cfd01362-a4c2-42b9-a617-c83082a289d7/Presentation/PublicationAttachment/891e6ada-3402-44d1-b1f7-b40c8f3af95a/Privacy\\_fallacy.pdf](https://www.huntonak.com/files/Publication/cfd01362-a4c2-42b9-a617-c83082a289d7/Presentation/PublicationAttachment/891e6ada-3402-44d1-b1f7-b40c8f3af95a/Privacy_fallacy.pdf). (“Granting data subjects property rights in all data pertaining to them fails to recognize that the person that collects the data makes investments in collecting and manipulating the data, thus creating economic value. Sophisticated data controllers use the data that they collect to generate new data.”)

<sup>92</sup> *Id.*, p. 8. (“Prioritizing data protection at the expense of legitimate uses that benefit citizens will forestall innovation. An optimal regulatory model would favor a nuanced approach where regulation is based on the nature and use of the data that enables legitimate business uses of personal data, fosters cross-border data flows, and empowers consumers to make informed choices. Moreover, data protection regulation must be a coherent streamlined set of rules that establishes clear authorities to minimize complexity.”)

---

<sup>93</sup> Ryan Hagemann and Alec Stapp, *Comments to the National Telecommunications and Information Administration in the Matter of: International Internet Policy Priorities*, Niskanen Center (Washington, D.C.; 17 July 2018), p. 9, <https://niskanencenter.org/wp-content/uploads/2018/07/Comments-International-Internet-Policy-NTIA.pdf>.

<sup>94</sup> Cameron F. Kerry, “Why protecting privacy is a losing game today—and how to change the game,” Brookings Institution (Washington, D.C.: 12 July 2018), <https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/>.

<sup>95</sup> *Id.*

<sup>96</sup> *Id.*

<sup>97</sup> Joshua New and Daniel Castro, *How Policymakers Can Foster Algorithmic Accountability*, Center for Data Innovation (Washington, D.C.: 21 May 2018), p. 9, <http://www2.datainnovation.org/2018-algorithmic-accountability.pdf>.

<sup>98</sup> *Id.*, pp. 9-10.

<sup>99</sup> Curt Levey and Ryan Hagemann, “Algorithms With Minds of Their Own,” *The Wall Street Journal*, 12 Nov. 2017, <https://www.wsj.com/articles/algorithms-with-minds-of-their-own-1510521093>. (“The machine’s ‘thought process’ is not explicitly described in the weights, computer code, or anywhere else. Instead, it is subtly encoded in the interplay between the weights and the neural network’s architecture. Transparency sounds nice, but it’s not necessarily helpful, and may be harmful.”)

<sup>100</sup> Kartik Hosanagar and Vivian Jair, “We Need Transparency in Algorithms, But Too Much Can Backfire,” *Harvard Business Review*, 25 July 2018, <https://hbr.org/2018/07/we-need-transparency-in-algorithms-but-too-much-can-backfire>.

<sup>101</sup> New and Castro, *supra* note 97 at 27-29.

<sup>102</sup> Bughin, et. al., *supra* note 32 at 6.