NISKANEN CENTER

Regulatory Comment

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

HEARINGS ON COMPETITION AND CONSUMER PROTECTION IN THE 21ST CENTURY

The Intersection Between Privacy, Big Data, and Competition

Alec Stapp
Technology Policy Fellow
Niskanen Center

Ryan Hagemann
Senior Director for Policy
Niskanen Center

Submitted: August 20, 2018
Docket Number: FTC-2018-0051

EXECUTIVE SUMMARY

Data is an important dimension of competition for platforms, but attention is the real scarce resource in the market. To capture attention and stay competitive in the market, companies identify customers' needs and preferences and create products that satisfy them. People say they value privacy, but they act like they don't. Research from behavioral economics shows that privacy valuation is highly context-dependent and subject to social-desirability bias and endowment effects.

Advocates want to increase privacy and competition, but there is an unacknowledged trade-off between those values. Privacy regulations are costly, ambiguous, and vague, which means they are biased in favor of incumbents and harmful to innovation. If we value privacy above all else, then that is a fine trade-off to make. But we should not pretend privacy regulations are a free lunch.

Federalism gives us the benefit of states serving as "laboratories of democracy,"[1] but at the cost of potential regulatory arms races. The "California effect" means that a single large state can, in effect, drive policymaking at the national level, creating a race to the bottom.[2] We should pass federal baseline privacy regulations that preempt state privacy laws.

INTRODUCTION

"Data is the new oil."[3] This metaphor has become a meme. It is reasonable that as the digital economy becomes more prominent in our lives, we would seek to understand one of its most important inputs by reaching for an analogy to the physical economy. But we should be careful not to think of data as a resource to be consumed, lest we regulate and manage it improperly.[4] There are a few ways this analogy leads us astray.

First, oil is rivalrous, while data is nonrivalrous. If someone uses a barrel of oil, it can't be consumed again. But as Alan McQuinn, a senior policy analyst at the Information Technology and Innovation Foundation, noted in an article for Inside Sources, "when consumers 'pay with data' to access a website, they still have the same amount of data after the transaction as before. As a result, users have an infinite resource available to them to access free online services."[5]

Second, oil is fungible, while data is nonfungible. One barrel of oil is the same as another, by its definition as a commodity. Data, on the other hand, is heterogeneous: each person's data is unique and there are many different types of attributes that can be turned into data. Third, oil has positive marginal costs of production and distribution, while data has near-zero marginal costs for both.

Lastly, oil is a search good (i.e., value can be assessed before purchase) while data is an experience good. Often, the value of data to a firm can only be determined after it's purchased and combined with other data (or put to use in proprietary algorithms).[6]

As author Bernard Marr suggests, a better analogy would be renewable energy.[7] Like data, the sources of renewable energy are all around us — the sun shining, rivers running, wind blowing — and there is more available than we could ever use. We just need to capture it, like we do with data. We leave our digital fingerprints everywhere; to turn them into data, we just need someone to dust them off.

PART I: DOES BIG DATA MEAN LITTLE COMPETITION?

Data as a dimension of competition, and/or as an impediment to entry into or expansion within a relevant market.

There is a common misconception that technology platforms with ad-based business models auction off their users' personal data to the highest bidder.[8] In fact, these platforms have an incentive not to sell private data — whether it was provided by the user or collected by the company observing user behavior.[9] User data is, in effect, a trade secret that they use to improve their advertising services.

The platforms use this data to facilitate targeted advertising, i.e., selling access to the attention of users in particular categories. For example, advertisers can target messages to Facebook users based on their location, demographics, interests, behavior, and connections.[10] Proprietary data is helpful in the advertising market, but the tech giants are not the only competitors with access to data.

As Anja Lambrecht, an assistant professor at London Business School, and Catherine E. Tucker, a professor at MIT Sloan School of Management, argue in a recent paper, for "big data" to provide a sustainable competitive advantage, it would need to be inimitable, rare, valuable, and nonsubstitutable. It fails on all counts.[11]

First, big data is neither inimitable nor rare. As discussed above, since data is nonrivalrous and has near-zero marginal costs, data owned by one firm can be replicated by a competitor. "Data brokers," such as Experian, Epsilon, and Acxiom, play an important role here. They sell data to their customers (who might not have proprietary datasets of their own) for targeted advertising campaigns, people searches, and risk mitigation via identity verification and fraud detection.[12] Advances in the on-demand cloud computing industry have also drastically reduced costs for computing, storing, and analyzing big data.

Lambrecht and Tucker point out three challenges to ensuring big data is valuable for firms: integrating new data into the business and making it compatible with pre-existing data; extracting value from unstructured data; and establishing causal relationships from the data. After reviewing these challenges, the authors conclude that "it is only when combined with managerial, engineering and analytic skill in determining the experiment or algorithm to apply to such data that it proves valuable to firms."[13]

Finally, the authors discuss cases when new entrants broke into markets where big data was supposed to have created an impenetrable moat, including WhatsApp in the communications market, King Digital Entertainment in the online gaming market, and Tinder in the online dating market. In the end, it's not the data that makes the difference, but the "superior ability to understand and meet customer needs."[14]

At a festival in Los Angeles last year, Reed Hastings, the CEO of Netflix, discussed his view of the competitive landscape:[15]

> *"Sometimes employees at Netflix think, 'Oh my god, we're competing with FX, HBO, or Amazon,' but think about if you didn't watch Netflix last night: What did you do? There's such a broad range of things that you did to relax and unwind, hang out, and connect — and we compete with all of that. You get a show or a movie you're really dying to watch, and you end up staying up late at night, so we actually compete with sleep."*

Hastings goes on to claim that Netflix is actually winning the competition against sleep. This might have been tongue-in-cheek, but his overarching point is only slightly hyperbolic: in the digital economy, data is important, but attention is the brass ring. People have a finite amount of time each day and the companies that create the best products and services win the competition for the real resource that is inimitable, rare, valuable, and nonsubstitutable: attention.

PART II: THE PRIVACY PARADOX

Competition on privacy and data security attributes (among, for example, social media companies or app developers), and the importance of this competition to consumers and users.

Whether consumers prefer free/ad-supported products to products offering similar services or capabilities, but that are neither free nor ad-supported.

There is a paradox at the heart of how people treat privacy. They say they value privacy while their actions imply they don't. In other words, their stated preferences contradict their revealed preferences. Is this just another example of cheap talk? Research from behavioral economics and related fields has shown that privacy valuations are highly context-dependent and subject to social-desirability bias and endowment effects.

People say they value privacy: According to a 2014 Associated Press-GfK poll, "more than 60 percent of respondents said they value privacy over antiterror protections."[16] But they act as if they don't: "Although 70 percent of online consumers say they are worried about online privacy … just 40 percent read website privacy

statements, and 82 percent would give personal information to new shopping sites in exchange for a chance to win $100 in a sweepstakes."[17]

In one experiment, researchers showed that "participants were willing to pay around fifty cents for increased privacy, yet were not willing to spend much more than a dollar, regardless of the nature of the item."[18] In another, the vast majority of participants were willing to reveal their monthly income to a video rental store in exchange for a 1€ discount on a DVD (without the discount, about half still shared this private information in exchange for no benefit).[19]

A different study found that most subjects would happily sell their personal information for just 25 cents, and almost all of them waived their right to shield their information.[20] A study in New Zealand found that while most respondents said they were very sensitive to privacy issues, fewer than half were willing to pay for property rights to their personal information. And of those willing to pay, the average amount was $28.[21]

The privacy "good" is often part of a complex bundle — for example, discounts at chain stores in exchange for using a loyalty card that tracks purchasing data.[22] According to a Deloitte survey, 79 percent of respondents "agreed that they would be willing to share their personal data if there was a clear benefit to them."[23]

Privacy valuations are also context-dependent.[24] In a summary of its 2016 survey, Pew said, "These findings suggest that the phrase that best captures Americans' views on the choice between privacy vs. disclosure of personal information is, 'It depends.' People's views on the key tradeoff of the modern, digital economy — namely, that consumers offer information about themselves in exchange for something of value — are shaped by both the conditions of the deal and the circumstances of their lives."[25]

Privacy has a "social-desirability bias" as well: People care much less about privacy if they perceive the information or behavior being tracked to be socially desirable. As one article puts it, "The less desirable the trait, the greater the price a person demands for releasing the information."[26] Privacy is also subject to an endowment effect: One experiment showed that those who started with more privacy protections were five times more willing to forgo money to preserve their privacy.[27] Given that few people are confident their records will remain private, it's therefore reasonable to conclude that the endowment effect makes people value privacy less.[28]

Do platforms compete on privacy? GoGoDuck, the search engine competitor to Google that prides itself in protecting users' privacy, has a market share of less than 1 percent in the United States.[29] But Facebook did end its data-sharing agreements with third-party data brokers after the Cambridge Analytica scandal caused a wave of negative publicity for the company.[30]

Based on their choices across a wide variety of products and services, consumers express a clear preference for free, ad-supported options. Android, the free, open-source mobile operating system developed by Google, had 85.9 percent of the global smartphone sales in 2017, while iOS had 14 percent.[31] None of the most popular social media platforms charge customers for access.[32]

PART III: WHAT PRICE PRIVACY?

The benefits and costs of privacy laws and regulations, including the effect of such regulations on innovation, product offerings, and other dimensions of competition and consumer protection.

There is a tradeoff between privacy regulations and economic dynamism. Policymakers who pass privacy regulations do so with good intentions, but these new mandates also come with unintended consequences.

It's important to keep in mind that while consumers value privacy, they also value choice, innovation, and affordability. Now that the General Data Protection Regulation (GDPR) has been implemented in the European Union and other jurisdictions are considering mirroring its approach to privacy, it's worth examining the law's effects.

European regulators adopted GDPR with the noble goal of mitigating privacy violations by bad actors. But many experts predicted ahead of time what the costs of this policy would be. Vague and ambiguous regulations also raise the cost of doing business. The rules are so difficult to interpret even the EU Parliament's own website may not be in total compliance.[33] This ambiguity contributes to GDPR's liability risks. Penalties from the European Union for violations are significant — up to 4 percent of an infringing company's total worldwide revenue— and any individual damaged by an infringement also has a private right of action for compensation.[34][35] Facebook and Google were hit with $8.8 billion in GDPR lawsuits on day one.[36][37] Compliance costs are also exorbitant: the 500 largest companies in the world will spend roughly $7.8 billion to make sure they don't run afoul of the new law.[38] The combination of fines, compliance costs, and legal liability make GDPR potentially crippling for all but the largest firms.

And the stakes are higher for privacy regulation in the United States than in Europe, given the global distribution of technology companies. The United States has the top five largest Internet companies in the world — Apple, Amazon, Microsoft, Google, and Facebook — and 11 of the top 20.[39] Europe has zero. Unclear privacy mandates could have tremendous costs if implemented in the United States, where the digital economy accounts for 6.5 percent of GDP and directly supports 5.9 million jobs.[40]

GDPR is particularly terrible for digital publishers. Following implementation, programmatic ad-buying decreased by as much as 25 to 40 percent in some cases.[41] The limitations on using data for ad targeting also reduce their effectiveness: "In Europe, where privacy laws have been implemented, banner ads have experienced a reduction in effectiveness of 65 percent on average in terms of changing stated purchase intent."[42] Most ominously, two months after GDPR took effect, more than 1,000 U.S. news sites are still unavailable in Europe.[43]

The new law is also bad for innovation. As my colleague Ryan Hagemann and I wrote in a recent op-ed:[44]

> *Unclearly defined provisions such as the "right to erasure" and "right to explanation," even if interpreted reasonably, are regulatory death blows for investments in many emerging technologies. The potential commercial applications of technologies such as blockchain and artificial intelligence are fundamentally incompatible with the new rules, (which) serve only to cement the EU's position as the technological backwater of the industrial world.*

It is tragically ironic that at a time when the European Union is using antitrust enforcement actions to punish large technology companies, European policymakers passed a privacy law that favors those same firms. Adam Thierer, a senior research fellow at the Mercatus Center at George Mason University, predicted before implementation that GDPR would further entrench Facebook and Google rather than reign them in.[45] As European Union Justice Commissioner Věra Jourová said after meeting with Google and Facebook and noting a lack of anxiety about GDPR, "They have the money, an army of lawyers, an army of technicians and so on."[46]

Hiawatha Bray, a technology columnist for *The Boston Globe*, admitted in a recent article about California's new GDPR-style law that though the increase in concentration may not be the intent of privacy regulation, it's not unwelcome either:[47]

Perhaps strong privacy regulations will prevent the rise of "the next Facebook," but is that a bad thing? Maybe new regulations will result in fewer companies hitting me up for sensitive data. But I'd rather have one or two huge companies tracking me than 20 or 30 smaller ones. There are fewer opportunities for data breaches that way, and it's easier to sue when something goes wrong.

Regulations intended to give people more control over their data, such as portability and interoperability requirements, actually pose cybersecurity risks. By increasing what experts call the "attack surface,"[48] or the number of points where a hacker could extract private information, these regulations directly increase the risk of users' private data being stolen or exposed. The Facebook-Cambridge Analytica scandal was really a case of data portability run amok. Facebook allowed its users to share their data (and some of their friends' data) with third-party developers and it ended up being used for political purposes.

PART IV: PREEMPTING THE CALIFORNIA EFFECT

The benefits and costs of varying state, federal and international privacy laws and regulations, including the conflicts associated with those standards.

A patchwork of varying state, federal, and international privacy laws creates a race to the bottom where the jurisdiction with the most onerous regulations becomes the de facto lawmaker for all jurisdictions. In environmental policy, this is known as the "California effect," a phrase coined by David Vogel, a professor at the University of California, Berkeley, after he observed that automakers would make all of their vehicles comply with California's pollution standards because the state was so large and a customized production process was too inefficient.[49]

California recently passed its own privacy law, which is essentially "GDPR lite."[50] Among its most troubling provisions, the law prohibits companies from providing customers with an inferior service if they choose to not share their data. But the data economy is premised on sharing data in exchange for free digital services. This particular regulation creates a classic free-rider problem in which no one has an incentive to provide their data, and therefore the underlying service will become uneconomical.[51]

The federal government should limit the damage from these state-level privacy laws and preempt them by passing its own baseline privacy law and invoking the Constitution's supremacy clause. The new law should maintain sector-based privacy regulations (e.g., HIPAA for health care, FERPA for education, and FCRA and GLBA for credit) and continue with an ex-post approach to privacy enforcement as opposed to the ex-ante approach favored in the EU. This strategy does an excellent job addressing real risks to sensitive data and real harms to consumers.

The federal privacy law should consider incorporating a few proposals from a recent white paper released by Senator Mark Warner of Virginia, including AI self-identification, platform liability for re-uploading of content deemed tortious by a court, 72-hour data-breach notifications, and transparency requirements for digital political ads.[52]

PART V: SUMMARY OF RECOMMENDATIONS

1. **Maintain sector-based privacy regulation for sensitive medical, educational, and financial information;**

2. **Preempt state regulation of online privacy by passing baseline federal privacy regulation that is predictable, minimalist, consistent, and simple;**

3. **Violations of privacy regulations should be adjudicated by the FTC, not in the court system via private lawsuits;**

4. **Platforms should be liable for harm if they fail to prevent content that has been deemed tortious by a court from being re-uploaded; and**

5. **Firms suffering a data breach should be required to notify affected users within 72 hours.**

CONCLUSION

There is a growing push for new privacy regulations, as seen with the recent passage of laws in California and the European Union. As the federal government and various agencies approach this issue and consider its effects for competition and other values, it would be wise to follow the template laid out in the Clinton administration's *Framework for Global Electronic Commerce*.[53] Though the framework was primarily concerned with commerce, its principles apply with equal force to privacy:

1. "The private sector should lead."

2. "Governments should avoid undue restrictions on electronic commerce."

3. "Where governmental involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent and simple legal environment for commerce."

4. "Governments should recognize the unique qualities of the Internet."

5. "Electronic commerce on the Internet should be facilitated on a global basis."[54]

We would like to thank the FTC for the opportunity to comment on this issue and we look forward to continuing to engage on this and other topics as the hearings progress.

[1] *New State Ice Co. v. Liebmann*, 285 U.S. 262 (1932).
[2] David Vogel, *Trading up: Consumer and Environmental Regulation in a Global Economy* (Harvard University Press, 2009).
[3] "The World's Most Valuable Resource Is No Longer Oil, but Data," *The Economist*, May 6, 2017, https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.
[4] Cornelius Puschmann and Jean Burgess, "Big Data, Big Questions| Metaphors of Big Data," *International Journal of Communication* 8 (2014): 20.
[5] Alan McQuinn, "No, Internet Users Are Not Paying With Their Data," InsideSources, August 7, 2018, http://www.insidesources.com/no-internet-users-not-paying-data/.
[6] MIT Technology Review Insights, "Data's Identity in Today's Economy," MIT Technology Review, accessed August 16, 2018, https://www.technologyreview.com/s/601207/datas-identity-in-todays-economy/.
[7] Bernard Marr, "Here's Why Data Is Not The New Oil," Forbes, accessed August 15, 2018, https://www.forbes.com/sites/bernardmarr/2018/03/05/heres-why-data-is-not-the-new-oil/.
[8] Daniel Castro, "Eight Things Congress Doesn't Get About Facebook" (Information Technology and Innovation Foundation, April 16, 2018), https://itif.org/publications/2018/04/16/eight-things-congress-doesnt-get-about-facebook.
[9] "Google Privacy | Why Data Protection Matters," accessed August 16, 2018, http://privacy.google.com/intl/en_ALL/how-ads-work.html.
[10] "Core Audiences," Facebook Business, accessed August 16, 2018, https://www.facebook.com/business/learn/facebook-ads-choose-audience.
[11] Anja Lambrecht and Catherine E. Tucker, "Can Big Data Protect a Firm from Competition?," 2015.
[12] Jeremy B. Merrill, "How to Wrestle Your Data From Data Brokers, Silicon Valley — and Cambridge Analytica," ProPublica, April 30, 2018, https://www.propublica.org/article/how-to-wrestle-your-data-from-data-brokers-silicon-valley-and-cambridge-analytica.
[13] Lambrecht and Tucker, "Can Big Data Protect a Firm from Competition?"
[14] Lambrecht and Tucker.
[15] Rina Raphael, "Netflix CEO Reed Hastings: Sleep Is Our Competition," Fast Company, https://www.fastcompany.com/40491939/netflix-ceo-reed-hastings-sleep-is-our-competition.
[16] "Poll Finds Americans Value Privacy over Security," BostonGlobe.com, accessed August 16, 2018, https://www.bostonglobe.com/news/nation/2014/01/28/poll-finds-americans-value-privacy-over-security/MQTZVLsZfO8AhJMiDsl5vK/story.html.
[17] Bob Tedeschi, "E-Commerce Report; Everybody Talks about Online Privacy, but Few Do Anything about It," *The New York Times*, June 3, 2002, sec. Business Day, https://www.nytimes.com/2002/06/03/business/e-commerce-report-everybody-talks-about-online-privacy-but-few-anything-about-it.html.
[18] Janice Y. Tsai et al., "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study," *Information Systems Research* 22, no. 2 (2011): 254–268.
[19] Alastair R. Beresford, Dorothea Kübler, and Sören Preibusch, "Unwillingness to Pay for Privacy: A Field Experiment," *Economics Letters* 117, no. 1 (2012): 25–27.
[20] Jens Grossklags and Alessandro Acquisti, "When 25 Cents Is Too Much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information," in *WEIS*, 2007.
[21] E. Rose, "Data Users versus Data Subjects: Are Consumers Willing to Pay for Property Rights to Personal Information?," in *Proceedings of the 38th Annual Hawaii International Conference On System Sciences* (IEEE, 2005), 180c–180c.
[22] Alessandro Acquisti and Jens Grossklags, "What Can Behavioral Economics Teach Us about Privacy," *Digital Privacy: Theory, Technologies and Practices* 18 (2007): 363–377.
[23] Gina Pingitore et al., "To Share or Not to Share," *Deloitte University Press*, n.d.
[24] Alessandro Acquisti, "The Economics of Personal Data and the Economics of Privacy," 2010.
[25] Lee Rainie and Maeve Duggan, "Privacy and Information Sharing," *Pew Research Center: Internet, Science & Tech* (blog), January 14, 2016, http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/.
[26] Bernardo A. Huberman, Eytan Adar, and Leslie R. Fine, "Valuating Privacy," *IEEE Security & Privacy* 3, no. 5 (2005): 22–25.
[27] Alessandro Acquisti, Leslie K. John, and George Loewenstein, "What Is Privacy Worth?" *The Journal of Legal Studies* 42, no. 2 (2013): 249–274.

[28] "Few Express Confidence That Their Records Will Remain Private and Secure," *Pew Research Center: Internet, Science & Tech* (blog), May 19, 2015, http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/pi_15-05-20_privacysecurityattd07/.
[29] "Search Engine Market Share," accessed August 16, 2018, https://netmarketshare.com/search-engine-market-share.aspx.
[30] "Facebook Limiting Information Shared With Data Brokers," *The Wall Street Journal*, March 28, 2018, https://www.wsj.com/articles/facebook-says-its-ending-use-of-information-from-outside-data-brokers-for-ad-targeting-1522278352.
[31] "Gartner Says Worldwide Sales of Smartphones Recorded First Ever Decline During the Fourth Quarter of 2017," accessed August 16, 2018, https://www.gartner.com/en/newsroom/press-releases/2018-02-22-gartner-says-worldwide-sales-of-smartphones-recorded-first-ever-decline-during-the-fourth-quarter-of-2017.
[32] "Top U.S. Mobile Social Apps by Users 2018 | Statistic," Statista, accessed August 16, 2018, https://www.statista.com/statistics/248074/most-popular-us-social-networking-apps-ranked-by-audience/.
[33] Matthias Gliwka, "EU Parliament Website Violates GDPR," *Matthias Gliwka* (blog), May 17, 2018, https://medium.com/matthias-gliwka/eu-parliament-websites-violates-gdpr-200eb2c00e8f.
[34] "Art. 83 GDPR – General Conditions for Imposing Administrative Fines," *General Data Protection Regulation*, accessed August 17, 2018, https://gdpr-info.eu/art-83-gdpr/.
[35] "Art. 82 GDPR – Right to Compensation and Liability," *General Data Protection Regulation*, accessed August 17, 2018, https://gdpr-info.eu/art-82-gdpr/.
[36] Russell Brandom, "Facebook and Google Hit with $8.8 Billion in Lawsuits on Day One of GDPR," The Verge, May 25, 2018, https://www.theverge.com/2018/5/25/17393766/facebook-google-gdpr-lawsuit-max-schrems-europe.
[37] "Art. 83 GDPR – General Conditions for Imposing Administrative Fines."
[38] "Global 500 Companies to Spend $7.8B on GDPR Compliance," accessed August 16, 2018, https://iapp.org/news/a/survey-fortune-500-companies-to-spend-7-8b-on-gdpr-compliance/.
[39] "Internet Trends Report 2018," Kleiner Perkins, accessed August 16, 2018, https://www.kleinerperkins.com/perspectives/internet-trends-report-2018.
[40] "Initial Estimates Show Digital Economy Accounted for 6.5 Percent of GDP in 2016," National Telecommunications and Information Administration, accessed August 16, 2018, https://www.ntia.doc.gov/blog/2018/initial-estimates-show-digital-economy-accounted-65-percent-gdp-2016.
[41] Jessica Davies, "GDPR Mayhem: Programmatic Ad Buying Plummets in Europe," *Digiday* (blog), May 25, 2018, https://digiday.com/media/gdpr-mayhem-programmatic-ad-buying-plummets-europe/.
[42] Avi Goldfarb and Catherine E. Tucker, "Privacy Regulation and Online Advertising," *Management Science* 57, no. 1 (2011): 57–71.
[43] Jeff South, "More than 1,000 U.S. News Sites Are Still Unavailable in Europe, Two Months after GDPR Took Effect," *Nieman Lab* (blog), accessed August 16, 2018, http://www.niemanlab.org/2018/08/more-than-1000-u-s-news-sites-are-still-unavailable-in-europe-two-months-after-gdpr-took-effect/.
[44] Ryan Hagemann and Alec Stapp, "The EU's Online-Privacy Boondoggle," *National Review*, June 27, 2018, https://www.nationalreview.com/2018/06/eu-online-privacy-regulations-a-disaster/.
[45] Adam Thierer, "How Well-Intentioned Privacy Regulation Could Boost Market Power of Facebook & Google," accessed August 16, 2018, https://techliberation.com/2018/04/25/how-well-intentioned-privacy-regulation-could-boost-market-power-of-facebook-google/.
[46] Sam Schechner and Nick Kostov, "Google and Facebook Likely to Benefit From Europe's Privacy Crackdown," *Wall Street Journal*, April 24, 2018, https://www.wsj.com/articles/how-europes-new-privacy-rules-favor-google-and-facebook-1524536324.
[47] Hiawatha Bray, "Calif.'s New Net Privacy Law Gives Consumers More Clout, and Big Tech May Be Just Fine with That," BostonGlobe.com, accessed August 16, 2018, https://www.bostonglobe.com/business/2018/07/01/calif-new-net-privacy-law-gives-consumes-more-clout-and-big-tech-may-just-fine-with-that/KAFKvsFHF9FNrzaODH21xL/story.html.
[48] "Attack Surface," *Wikipedia*, August 9, 2018, https://en.wikipedia.org/w/index.php?title=Attack_surface&oldid=854227979.
[49] David Vogel, "Environmental Regulation and Economic Integration," *Journal of International Economic Law* 3, no. 2 (2000): 265–279.

[50] Daisuke Wakabayashi, "California Passes Sweeping Law to Protect Online Privacy," *The New York Times*, accessed August 17, 2018, https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html.
[51] "ITIF Speaks Out Against California Privacy Law, Calls for Federal Privacy Legislation" (Information Technology and Innovation Foundation, June 29, 2018), https://itif.org/publications/2018/06/29/itif-speaks-out-against-california-privacy-law-calls-federal-privacy.
[52] Hanna Kozlowska, "This Paper Shows Just How Unprepared the US Is to Deal with the Problems Technology Has Created," Quartz, accessed August 17, 2018, https://qz.com/1345888/mark-warners-white-paper-outlines-how-unprepared-the-us-is-to-deal-with-problems-created-by-technology/.
[53] White House, *A Framework for Global Electronic Commerce*, (1997), https://clintonwhitehouse4.archives.gov/WH/New/Commerce/summary.html.
[54] *Id.*