PREPARED REMARKS

"Keep It: Maintaining Competition in the Privacy Debate"

Noah Joshua Phillips
Commissioner
U.S. Federal Trade Commission

July 27, 2018
Internet Governance Forum USA
Washington, D.C.

Thank you for the kind introduction, Steve. I would like to thank the Internet Governance Forum USA for hosting me today and for convening policy makers, thought leaders, and others to discuss privacy and other important Internet policy issues. I'm pleased to be here with all of you.

Let me begin by saying that the remarks I give today are my own and do not necessarily reflect the views of the Federal Trade Commission or any of my fellow Commissioners.

The FTC enforces both competition and consumer privacy law, so it is inevitable that, in thinking about one, we consider the other. More than inevitable, though, it is essential. When we evaluate changes in privacy law internationally, or consider the whether and how of privacy legislation here in the United States, competition must be part of that discussion. This is a distinct question from whether values associated with privacy ought to bear on antitrust analysis—a topic for another day.[1]

[1] *Cf.* James C. Cooper, *Privacy and Antitrust: Underpants Gnomes, the First Amendment, and Subjectivity*, 20 GEO. MASON L. REV. 1129 (2013).

I want today to register my concern that laws and regulations intended to promote privacy may build protective moats around large companies (some of which already possess significant amounts of data about people) by making it more difficult for smaller companies to grow, for new companies to enter the market, and for innovation to occur—and insist that competition be part of our conversation about privacy.

I am not alone in this. My good friend Caroline Holland—now an advisor to one of my fellow commissioners—wrote recently that "progress on one front [privacy] might lead to regression on the other [competition]."[2] Joe Simons, Chairman of the FTC, put it this way in testimony last week—paraphrasing slightly: "if you do privacy in the wrong way . . . , you might end up reducing competition. [¶] You might create a situation in which you entrench the large tech platforms . . . [and] make it very difficult for . . . new entrants and smaller firms to get the attention of the consumers that they're trying to reach."[3]

If our concern is warranted, the questions for proponents of new privacy rules then must include: Are we willing to allow a reduction in competition or innovation? What competitive price are we willing to pay for greater privacy protection? Are we

---

[2] Caroline Holland, *We Hope the Facebook Cambridge Analytica Scandal Will Improve Privacy Protections—But Could the Fallout Harm Competition?*, MEDIUM (May 3, 2018), https://medium.com/read-write-participate/we-hope-the-facebook-cambridge-analytica-scandal-will-improve-privacy-protections-but-could-the-a1ef9a246afb.

[3] *Oversight of the Federal Trade Commission: Hearing Before the Digital Com. & Consumer Protection Subcomm. of the H. Energy & Com. Comm.*, 115th Cong., Prelim. Tr. at 59-60 (July 18, 2018) (testimony of Joseph J. Simons, Chairman of the U.S. Fed. Trade Comm'n.), https://docs.house.gov/meetings/IF/IF17/20180718/108560/HHRG-115-IF17-Transcript-20180718.pdf.

willing, for instance, to allow the biggest technology companies—lately the focal points of discussion about both privacy and competition—to entrench further?

I suspect that this audience is already familiar with the various privacy and data security rules that apply in the U.S., but for those who may read this speech later—both of you—I want to set the stage.

The FTC has long been the federal agency with primary responsibility for and experience in privacy policy and enforcement. It has been 20 years since our first major online privacy case, against a company called GeoCities.[4]

A quick experiment: Raise your hand if you remember GeoCities. For those who don't, when I was in college, it was a popular web hosting service and one of the most common sites users would go to in order to access the World Wide Web. In 1999—the year after the FTC sued—GeoCities sold to Yahoo!, then a dominant player in search. (That all tells you a little bit about the history of competition on the Internet.) At any rate, 20 years ago, the FTC sued GeoCities for engaging in "deceptive practices in connection with its collection and use of personal identifying information ["PII"] from consumers", including, among other things, falsely telling users that their PII would only be used to provide them with the advertising, offers,

[4] *See* Complaint, *In the Matter of GeoCities*, Dkt. No. C-3850 (F.T.C. Aug. 13, 1998), *available at* https://www.ftc.gov/enforcement/cases-proceedings/982-3015/geocities.

or products and services they requested, when, in fact, GeoCities sold that information to third parties.[5]

The FTC brought the Geocities privacy suit nearly 30 years after the passage of one of the nation's first and most significant data privacy laws, the Fair Credit Reporting Act,[6] which, among other things, regulates the sharing of consumer information by credit bureaus. As the Supreme Court explained, FCRA was passed for the dual goals of "promot[ing] efficiency in the Nation's banking system and [ ] protect[ing] consumer privacy."[7] Since then, Congress has passed an array of privacy and data security laws and has directed the FTC (and other agencies) to develop a host of new rules—including updates to FCRA—governing the collection, use, sharing, and security of personal information.[8]

I won't bore you with a recitation of every privacy statute and rule we enforce, but the point is we have significant enforcement authority across a variety of commercial privacy areas.[9] And other federal agencies enforce other privacy

---

[5] Analysis of Proposed Consent Order to Aid Public Comment, *In the Matter of GeoCities*, Dkt. No. C-3850 (F.T.C. Aug. 13, 1998) ("[T]he complaint alleges that GeoCities[, among other things,] falsely represented that the personal identifying information it collects through the membership application form is used only to provide members the specific advertising offers and products or services they request. In fact, according to the complaint, that information has been sold, rented or otherwise disclosed to third parties who have used it for purposes other than those for which members have given permission."), *available at* https://www.ftc.gov/enforcement/cases-proceedings/982-3015/geocities.

[6] 15 U.S.C. §§ 1681-1681x.

[7] *TRW Inc. v. Andrews*, 534 U.S. 19, 23 (2001).

[8] For example, Congress passed the Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), which amended FCRA and, among other things, directed the FTC and other federal agencies to develop regulations relating to identity theft detection programs. *See* Pub. L. No. 108-159, 117 Stat. 1952 (2003); 15 U.S.C. § 1681m. The FTC's "Red Flags" rule is codified at 16 C.F.R. pt. 681.

[9] *See, e.g.*, Children's Online Privacy Protect Act of 1998 ("COPPA"), 15 U.S.C. §§ 6501-6506; Children's Online Privacy Protection Rule, 16 C.F.R. pt. 312; Financial Privacy Rule, 16 C.F.R. pt. 313; Safeguards Rule, 16 C.F.R. pt. 314.

laws,[10] such as HIPAA,[11] the reason you have so much to do at the doctor's office other than seeing your doctor.

This all is not an accident of history, as some would have you believe. When you step back, what becomes clear is that we in the U.S. have a principled, risk-based approach that focuses privacy and security rules on the sectors of the economy where Congress has determined such rules are most needed. Even within those sectors, our approach recognizes that all entities are not the same, and, in many cases, the law explicitly permits different types of protections based on the size of the entity, the data being protected, and the like.

The United States' risk-based approach imposes the greatest costs on businesses at the points where our democratic process has determined the greatest privacy need exists, limiting such costs where the need is less. So, while we may argue about whether the risks are being appropriately evaluated, whether "leveling the playing field" among firms doing different things with different kinds of data makes sense, or whether the quantity and quality of data being collected today ought to change our approach, we should not be confused about whether the American approach to privacy is deliberate or sensible.[12]

---

[10] *See, e.g.*, Health Insurance Portability and Accountability Act ("HIPAA") Privacy Rule, 45 C.F.R. pts. 160 and 164, which is overseen by the Department of Health and Human Services; Family Educational Rights and Privacy Act of 1974 ("FERPA"), 20 U.S.C. § 1232g, and its implementing regulations, 34 C.F.R. pt. 99, which are overseen by the Department of Education.

[11] HIPAA, 42 U.S.C. § 1320d-2 note (Recommendations With Respect to Privacy of Certain Health Information).

[12] *See, e.g.*, Alessandro Acquisti, Curtis Taylor, & Liad Wagman, *The Economics of Privacy*, 54 J. ECON. LITERATURE 442, 478 (2016) ("[R]ather than a uniform piece of regulation to address contemporary privacy issues, a nuanced approach—dynamic and individualized to specific markets, contexts, and scenarios—may be necessary.").

The American approach stands in contrast to the privacy regime now in place in Europe, and the one set to become effective in California in 2020. Fundamentally, these regimes require everybody to adhere to one set of standards (and one set of costs) that apply to all online entities—regardless of size, regardless of service, regardless of risk.

What might be the cost of such an approach to privacy? By their nature, regulatory regimes create compliance costs that are durable and may become more onerous over time. These are what economists call "economies of scale", costs that large companies can bear more easily than their smaller competitors or new entrants.[13] Don't take it from me. As Mark Zuckerberg told Congress, "I think, a lot of times, regulation, by definition, puts in place rules that a company that is larger, that has resources like ours, can easily comply with, but that might be more difficult for a smaller start-up to [ ] comply with."[14] I should note that, in the same testimony, he signaled his openness to additional regulation.[15] While we may want to protect privacy in new ways, we do not want the regulatory burden to be so

---

[13] *See, e.g.*, William A. Brock & David S. Evans, *The Economics of Regulatory Tiering*, 16 RAND J. ECON. 398, 399 (1985) ("[I]mposing uniform regulatory requirements across all types of businesses has a disparate impact on smaller businesses because there are scale economies in regulatory compliance. Scale economies may arise because there are fixed costs of complying with regulations. Larger businesses can average these fixed costs over a larger quantity of output and thereby achieve a competitive advantage over their smaller rivals. [¶] There is evidence that scale economies in compliance are quite extensive for some regulatory requirements.") (citations omitted).

[14] *Transcript of Zuckerberg's appearance before House committee*, WASH. POST (Apr. 11, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/04/11/transcript-of-zuckerbergs-appearance-before-house-committee/?utm_term=.2952d85fa38f.

[15] *Id*. ("[T]he Internet is growing in importance around the world in people's lives, and I think that it is inevitable that there will need to be some regulation. So my position is not that there should be no regulation. But I also think that you have to be careful about what regulation you put in place . . . ."); *see also id*. (agreeing that additional oversight "deserves a lot of consideration" and noting that he is "not the type of person who thinks that there should be no regulation, especially because the Internet is getting to be so important in people's lives around the world").

onerous that it excludes potential market entrants or inhibits innovation;[16] at the very least, we need an honest discussion about the costs and benefits.

Take the General Data Protection Regulation ("GDPR"), the new European privacy law. For Europeans, it represents an expression in law of their view that the protection of personal data is a fundamental right.[17] For the U.S., it may provide a test case for how a different privacy regime than our own might work. My concern is that early signs point to precisely the effects on competition that I fear. According to the Wall Street Journal, when the European Union's justice commissioner met with large technology companies prior to implementation, instead of hearing the complaints she reportedly expected, the companies told her that they would be compliant.[18] She explained: "They have the money, an army of lawyers, an army of technicians and so on."[19] Facebook, for example, "mobilized hundreds of people in what it describes as the largest interdepartmental team it has ever assembled."[20] Jedidiah Yueh wrote in Forbes: "[i]ronically, big tech companies such as Facebook, Amazon, Apple and Google benefit from a silver lining when it

---

[16] James Campbell, Avi Goldfarb, & Catherine Tucker, *Privacy Regulation and Market Structure*, 24 J. ECON. & MGMT. STRATEGY 47, 47 (2015) ("Our results suggest that the commonly used consent-based approach may disproportionately benefit firms that offer a larger scope of services. Therefore, though privacy regulation imposes costs on all firms, it is small firms and new firms that are most adversely affected. . . . [T]his negative effect will be particularly severe for goods where the price mechanism does not mediate the effect, such as the advertising-supported Internet.").

[17] General Data Protection Regulation, Commission Regulation (EU) 2016/679 of Apr. 27, 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, ¶¶ 1-5.

[18] Sam Schechner & Nick Kostov, *Google and Facebook Likely to Benefit from Europe's Privacy Crackdown*, WALL ST. J. (Apr. 23, 2018, 10:18 PM), https://www.wsj.com/articles/how-europes-new-privacy-rules-favor-google-and-facebook-1524536324.

[19] *Id*.

[20] *Id*.

comes to being regulated—what hurts their competitors more only makes them stronger."[21] That's not ironic—it's economic, exactly how economies of scale work. Resources devoted to compliance can be scaled, and could have been spent on innovation, wages, and so on.[22]

Beyond the standard economies of scale, privacy rules in particular may skew to benefit large incumbents. Consider requiring affirmative user consent, and assume that consumers are considering the question and being selective with whom they share information. Consumers are more likely to trust the companies they know. This is an application of what economists call "brand effect". And, to the extent large incumbents also provide popular services—for instance as a result of the network effects endemic to certain technology markets—the big guys win again.

On May 25—the date GDPR went live—the Wall Street Journal reported that some digital advertising—"ad tech"—companies (relatively small competitors to the large technology companies that dominate online advertising) decided to stop operating in Europe, due to the consent requirement.[23] "[A]dvertisers", according to the Journal, "[we]re planning to shift money away from smaller providers and

---

[21] Jedidiah Yueh, *GDPR Will Make Big Tech Even Bigger*, FORBES (June 26, 2018, 7:15 AM), https://www.forbes.com/sites/forbestechcouncil/2018/06/26/gdpr-will-make-big-tech-even-bigger/#350c37922592.

[22] *See, e.g.*, Julia Powles, *The G.D.P.R., Europe's New Privacy Law, and the Future of the Global Data Economy*, NEW YORKER (May 25, 2018) ("'For large multinationals, the staffing can be three hundred to five hundred people working on G.D.P.R. compliance,' [Jim Halpert, who handles privacy and cybersecurity issues at the law firm D.L.A. Piper] told me. 'The effort and expense is huge—big companies are easily spending over fifty million dollars in preparation.' Like all the other practitioners I spoke with, Halpert considers companies such as Google and Facebook easily capable of absorbing the law's requirements. 'It favors companies that are organized and capable of great expenditure,' he said."), https://www.newyorker.com/tech/elements/the-gdpr-europes-new-privacy-law-and-the-future-of-the-global-data-economy.

[23] Schechner & Kostov, *supra* note 18.

toward Google and Facebook . . . ."[24] Bill Simmons, co-founder and chief technology officer of Dataxu, a Boston-based ad tech company noted the paradox: "'GDPR is actually consolidating the control of consumer data onto these tech giants.'"[25] Snap's CEO also has recognized this point about GDPR, stating: "There are times in history when regulation has actually entrenched big companies because they're the most capable of complying. I think that's a huge mistake, because I think that that would inhibit innovation."[26]

There is another, more insidious, effect that any regulatory regime can have: large companies can manipulate legal requirements to their own benefit more easily than smaller competitors or new entrants.[27] Public choice theory teaches us that the durability of legislative and regulatory barriers to entry is one of the reasons that incumbents find it attractive to spend resources on securing legislation and regulation that insulate them from competition.[28] But the benefit to incumbents is not just lobbying for laws that favor them; it is also implementing seemingly

---

[24] *Id.*; *see also* Douglas MacMillan, *Google Blasts Through Hurdles*, WALL ST. J., July 24, 2018, at A6 ("[GDPR] may have even benefited Google by making its offerings more appealing than those of smaller players in the market. [¶] 'It was a safe choice to buy [advertising] using Google's tools and inventory,' [Brian] Wieser[, of the equity research company Pivotal Research Group,] said").

[25] Schechner & Kostov, *supra* note 18.

[26] Yueh, *supra* note 21.

[27] James B. Bailey & Diana W. Thomas, *Regulating Away Competition: The Effect of Regulation on Entrepreneurship and Employment*, 52 J. Reg. Econ. 237, 238 (2017) ("Knowing the ins and outs of a specific regulatory framework that governs a particular industry represents a fixed cost of doing business that can be difficult for new entrants to an industry to overcome") (citation omitted).

[28] *See generally* U.S. Fed. Trade Comm'n, *Policy Perspectives: Competition and the Regulation of Advanced Practice Nurses* (Mar. 2014), *available at* https://www.ftc.gov/reports/policy-perspectives-competition-regulation-advanced-practice-nurses; George J. Stigler, *The Theory of Economic Regulation*, 2 J. ECON. & MGMT. SCI. 3, 13-14 (1971); Gordon Tullock, *The Welfare Costs of Tariffs, Monopolies, and Theft*, 5 W. ECON. J. 224 (1967); MILTON FRIEDMAN, CAPITALISM AND FREEDOM 142-43 (U. Chi. Press, 1962).

neutral laws or regulations in ways that benefit them at the expense of their would-be competitors. I don't think this is behind GDPR, California's law, or anything Congress might consider. But it does happen and it is concerning.

I'm also concerned about stifling innovation. Several papers have analyzed the effect of state privacy laws on the adoption of electronic medical records ("EMRs"), which not only make the exchange of information more efficient but can also lead to improvements in the quality of care.[29] The authors find that these laws "significantly reduced the adoption of [EMRs]"[30]—evidence that privacy regulations have inhibited the proliferation of innovative technologies that benefit consumers, in this case patients. And if the healthcare analogy holds, a poorly designed national privacy regime could impose higher compliance costs across the economy, hindering innovation and increasing barriers to entry.[31]

Finally, we may face still more unintended consequences. As Mr. Zuckerberg recently noted, "I think that the alternative [to the big U.S. technology companies], frankly, is going to be the Chinese companies."[32] He may have a motive in saying

---

[29] *See, e.g.*, Acquisti, Taylor, & Wagman, *supra* note 12, at 469 (summarizing the scholarship of Amalia R. Miller & Catherine E. Tucker).

[30] *Id*.

[31] *See, e.g.*, Samuel Waxman, Behnam Dayanim, & Brooke Schachner, *Legal health isn't easy for digital health companies*, TECHCRUNCH (Apr. 13, 2016) ("As the convergence of healthcare and technology continues, technology companies (and investors) are increasingly finding themselves lost in a thicket of unique legal issues, enforced by unfamiliar regulators, including privacy of patient information, consumer protection and fraud and patient safety. . . . Ensuring compliance with HIPAA can present both technical and administrative issues, especially for startups."), https://techcrunch.com/2016/04/13/legal-good-health-isnt-easy-for-digital-health-companies/; *see also* Austin Frakt, *The Astonishingly High Administrative Costs of U.S. Health Care*, N.Y. TIMES (July 16, 2018), https://www.nytimes.com/2018/07/16/upshot/costs-health-care-us.html.

[32] Kara Swisher, *Zuckerberg: The Recode Interview*, RECODE (July 18, 2018, 11:02 AM), https://www.recode.net/2018/7/18/17575156/mark-zuckerberg-interview-facebook-recode-kara-swisher.

that, but Chinese tech competition is real—indeed, it is China's national industrial policy—and may pose more than a competitive threat—something the Ranking Democrat on the Senate Select Committee on Intelligence, Mark Warner, has also recognized.[33]

The upshot is that, as we consider the potential benefits of new privacy protection, we must consider the costs, too: on competition and innovation. GDPR provides us with a great opportunity to see how a large-scale privacy regime works in practice, and for us in the United States to learn from Europe's experience. We don't yet know the answer. About the American risk-based approach, however, we can say one thing for certain already: it has both targeted the areas of greatest privacy need and still permitted a tremendous amount of innovation.

The upcoming hearings hosted by the FTC will also provide a good opportunity to discuss the important topic of how privacy is related to competition and innovation.[34] I invite everyone here to join and to weigh in with comments and proposals for those hearings.

Thank you very much.

---

[33] David McCabe, *Tech Giants' New Defense: Our Chinese Rivals Are Worse*, AXIOS (July 20, 2018) ("'I think this is worthy of some debate,' top Senate Intelligence Committee Democrat Mark Warner said last month to Axios, speaking about breaking up Facebook and other large tech players. 'One of my hesitancies, though, would be if we kneecapped American companies and they were simply replaced by Chinese tech companies. These are global companies now with global reach and we should tread softly.'"), https://www.axios.com/tech-giants-new-defense-our-chinese-rivals-are-worse-zuckerberg-aa1a2e5c-6aa6-45b3-aa2b-8217b792d10e.html.

[34] *See* Press Release, U.S. Fed. Trade Comm'n, *FTC Announces Hearings on Competition and Consumer Protection in the 21st Century* (June 20, 2018), https://www.ftc.gov/news-events/press-releases/2018/06/ftc-announces-hearings-competition-consumer-protection-21st.