UNITED STATES OF AMERICA
Federal Trade Commission

Opening Keynote of Commissioner Noah Joshua Phillips[1]

Privacy Regulation: Why, What, and When?
The Free State Foundation

Washington, DC
June 26, 2019

Thank you, Randy, for the warm introduction and the invitation to speak here today. The Free State Foundation's mission of using research and educational activities to promote understanding of free market, limited government, and rule of law principles is critical, and I am pleased to be here with you.

Today's event could not be timelier. We are in the midst of a robust debate, nationally and internationally, about consumer data privacy. I could talk all day about this topic, but, fortunately for everyone, Randy has limited me to about 15 minutes. With that in mind, I would like to highlight my top priorities for privacy legislation, taking advantage of the framework reflected in the title of today's seminar – "Privacy Regulation: Why, What, and When?" I can't speak to the "When" of privacy legislation, so I am going to diverge a bit and instead discuss the "How".

Let's start with "Why" we should consider privacy legislation. I see two reasons, above all. First, privacy violations can result in real and legally-cognizable consumer harms. Using its organic Section 5 authority and statutes like the Fair

[1] 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.

Credit Reporting Act and the Children's Online Privacy Protection Act, the Federal Trade Commission ("FTC") has a long history of protecting consumer privacy. Consumers and firms have increased dramatically the amount and use of data in the economy in recent years, so I think it is fair for lawmakers to contemplate whether our current framework necessitates additional, or perhaps overarching, privacy legislation, to address other identifiable privacy harms. Congress may also wish to address the perception of harms – warranted or not – from a sense that the collection and use of data are too complex, or simply go too far, which alone can influence marketplace behavior. The FTC has the dual mission of protecting consumers and fostering competition in broad sectors of the economy, which includes primary responsibility for protecting consumers' privacy. With those interests in mind, I think it is important that practices and conduct that harm consumers and thwart innovation and competition in the marketplace are identified, analyzed, and if need be, regulated.

Second, policy-makers around the world are training their focus on privacy. Domestically, the potential proliferation of state privacy laws, such as the California Consumer Privacy Act, will pose a host of challenges for companies large and small.[2] Europe has not only adopted the General Data Protection Regulation ("GDPR") but is using adequacy determinations and other tools to encourage other countries to follow suit. Europe and the U.S. differ in how we have approached privacy regulation, reflecting different philosophies and legal traditions, which lead

[2] For a comparison of state privacy legislation and laws, see Mitchell Noordyke, *US state comprehensive privacy law comparison*, IAPP PRIVACY TRACKER (Apr. 18, 2019), https://iapp.org/news/a/us-state-comprehensive-privacy-law-comparison/.

to different privacy regimes, and different tradeoffs. The European approach begins with fundamental rights in data, whereas we have looked to protect consumers from harm. I think it is crucial for the U.S. to keep its foothold and maintain an active role in the international arena. Privacy legislation incorporating our traditional harm-focused, risk-based approach to privacy protection might be one way to do so.

The "What" of privacy regulation is much more complicated. Privacy is a nebulous concept, and people differ as to whether and to what extent they experience a given kind of conduct as a violation. Are privacy harms limited to physical injury and financial loss? Do they include emotional distress? Is a sense of surveillance or creepiness characteristic of an eggshell plaintiff, or something Congress needs to prevent? What about a lack of empowerment or a loss of control? And how, if at all, do these things take us back to Brandeis and Warren's famous articulation of the Right to Privacy, the "right to be let alone"?[3]

Our Founders designed a republican form of government to answer questions like these. As Justice Gorsuch reminded us last week, "[t]he Constitution promises that only the people's elected representatives may adopt new federal laws restricting liberty".[4] Regulation restricts liberty, optimally only when the public good is advanced. That is why, as I have told Congress, it is the Legislature that needs to determine which harms need to be vindicated because privacy legislation will necessarily involve value judgements that should be left to it, not unelected Commission officials. What harms we address, what rights consumers ought to have

[3] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).
[4] Gundy v. United States, No. 17-6086, at *24 (U.S. June 20, 2019) (Gorsuch, J., dissenting).

to address those wrongs, are fundamental, non-delegable, democratic judgments. To be clear, that is not to say that the FTC doesn't have a role – any legislation that Congress determines to enact should maintain the FTC's role as the nation's primary privacy enforcement agency.

In considering whether and what to do, Congress will not be acting in a vacuum. Legislators can draw from our history and experience with our current risk-based privacy framework. Furthermore, the United States has already been working with our economic allies on privacy issues for decades – for instance, in the forms of the Privacy Frameworks of the Organization for Economic Cooperation and Development ("OECD") and the Asia-Pacific Economic Cooperation forum ("APEC") – and these can and should form a basis for the discussion.

Privacy legislation will involve tradeoffs, in particular when it comes to innovation and competition. Large companies can more easily bear the costs of compliance, while smaller entities will face more risk and uncertainty. That means that legislation carries the possibility of entrenching incumbents while limiting new market entrants who may provide competition and innovative, valuable products and services.

This is an issue that I have spoken about before,[5] and have raised with Congress. There is already some evidence that, since the implementation of GDPR,

[5] Commissioner Noah Joshua Phillips, *Keep It: Maintaining Competition in the Privacy Debate* (July 27, 2018), https://www.ftc.gov/public-statements/2018/07/keep-it-maintaining-competition-privacy-debate.

investment in startups is down in Europe[6] and more market share is flowing to the largest companies.[7] Time will tell about that impact.[8] To guard against these concerns, as Congress moves forward to regulate so much of the economy, it should take care and be cognizant about the impacts and tradeoffs. This means moving cautiously and learning from our experience with U.S. privacy laws in force today, and the experiences of jurisdictions that have instituted different privacy rules.

In considering legislation, one area Congress should focus on is information asymmetry, helping ensure that the market, and consumers in particular, have more, and more accessible, information on which to make informed decisions. One clear line we can draw to Brandeis is that "sunlight is said to be the best of disinfectants",[9] and better information can solve a host of problems. I also believe there is value in encouraging companies with large and complex data holdings and practices to engage in internal privacy assessments so that they better understand their own landscape and can make informed, risk-based decisions about how they gather, use, and share data.

For what it's worth, I think GDPR does offer some important concepts to consider. Take, for instance, determining democratically a set of legitimate data

---

[6] Jian Jia, Ginger Jin & Liad Wagman, *The short-run effects of GDPR on technology venture investment*, VOX EU (Jan. 7, 2019), https://voxeu.org/article/short-run-effects-gdpr-technology-venture-investment.
[7] Björn Greif, *Study: Google is the biggest beneficiary of the GDPR*, CLIQZ (Oct. 10, 2018), https://cliqz.com/en/magazine/study-google-is-the-biggest-beneficiary-of-the-gdpr.
[8] *See, e.g.*, Nick Kostove & Sam Schechner, *GDPR Has Been a Boon for Google and Facebook*, WALL ST. J. (June 17, 2019), https://www.wsj.com/articles/gdpr-has-been-a-boon-for-google-and-facebook-11560789219.
[9] Louis D. Brandeis, *What Publicity Can Do*, HARPER'S WKLY., Dec. 20, 1913, at 10.

uses where companies are free to operate, where even consent is not necessary. That approach can be efficient and makes economic sense.

One hears a lot of talk these days about rulemaking, penalty authority, preemption, and private rights of action. Those are important issues. But they are also secondary, in the sense that they are mechanisms to effectuate the will of Congress, to apply it and enforce it. So this process must involve first defining what the standard of liability should be and then deciding how best to effectuate it. Which brings us to the "How" of privacy legislation.

The first "How" is rulemaking. Rulemaking authority raises the important issues of delegation and democratic accountability that I mentioned earlier. Congress, not an administrative agency, is the best place to make policy with a profound impact on a substantial portion of the economy. Congress should consider that the flexibility that rulemaking permits also allows for changes in rules over time, which—regardless of the underlying policy—can be terrifically difficult for businesses attempting to adapt. A better strategy is to draft statutes that provide guidance on rulemaking to ensure that agencies effectuate congressional intent.

Another "How" of privacy legislation is the consideration of a civil penalty framework. The privacy legislation Congress is now considering may address many privacy harms that not only result in little to no tangible consumer harm, but also are much more difficult to quantify. Penalties can provide an important deterrent for bad conduct. But improperly calibrated penalties can deter companies from

exploring innovative and consumer-friendly products and services; the risk may simply be too great. Even properly calibrated enforcement can impose costs.

To account for this, any penalty scheme set by Congress should be built around the harms Congress defines and balance a range of factors, including consumer harm, and be set on a graduated scale, so as to tether them to coherent set of principles set out by Congress. A substantial body of economic literature supports the consideration of harm in the fashioning of penalties,[10] and common sense as well dictates that we punish more that which threatens more and worse harm. Furthermore, even if Congress is to impose penalties for initial violations, that scheme need not apply to every violation. Civil penalties could be foregone in the first instance for some conduct, particularly conduct the legality of which is more difficult to determine in the abstract and the deterrence of which may have negative consequences.

Preemption is another aspect of the "How" of privacy legislation. Application of a single legal framework across the country provides consistency and fairness. Allowing different states to apply different laws – the content of which we do not and cannot yet know – could result in different regimes in different states, and,

---

[10] That the state should set penalties equal to consumer harm (inflated by a factor to account for lack of perfect detection and prosecution) to maximize welfare is a standard result in economics dating back at least to Nobel Laureate Gary Becker's seminal work. *See* Gary S. Becker, *Crime & Punishment: An Economic Approach*, 76 J. POL. ECON. 169 (1968). The intuition behind this result is that setting penalties equal to harm forces actors to internalize the external costs they foist on society, which creates incentives to engage only in activities that generate net social benefits. *See, e.g.*, STEVEN SHAVELL, FOUNDATIONS OF ECONOMIC ANALYSIS OF LAW 474-79 (2004); Mitchell A. Polinsky & Steven Shavell, *Should Liability be Based on the Harm to the Victim or the Gain to the Injurer?*, 10 J.L. ECON. & ORG. 427 (1994); Louis Kaplow, *Optimal Deterrence, Uninformed Individuals, and Acquiring Information about Whether Acts are Subject to Sanctions*, 6 J.L. ECON. & ORG. 93 (1990). *See also* Richard Craswell, *Deterrence and Damages: The Multiplier Principle and Its Alternatives*, 97 MICH. L. REV. 2185, (1999).

accordingly, radically different goods and services offered by technology companies. Researchers have found that state-level privacy laws, built on top of a federal "floor" of regulation, have deterred the pro-consumer potential of electronic medical records.[11] A patchwork of different regulations will favor large, national, firms; and disproportionately hurt smaller operators, many of which may be local. In some cases, technology companies may choose not to provide certain services to citizens of some states because of the undue legal and financial risks a particular state's laws would impose. A single federal law could help avoid such outcomes and ensure that consumers across the country are treated fairly and equally.

Where we have a variety of differing state laws, the FTC will have to engage in competing investigations and lawsuits with state law enforcement agencies, rather than more efficient collaborations. The result will be less federal-state cooperation and more protracted investigations, more complicated litigation, and more challenging settlement environments. We may also face situations where similar – yet distinct – laws are subject to different legal interpretations by courts, removing some of the Commission's power to help shape consistency in that interpretation through our own case selection and legal arguments in federal court.

Let me finish with two final points. First, Attorneys General can be important partners in protecting consumers, acting as force multipliers for federal law enforcement. I think Congress should consider them. It should also consider

[11] *See, e.g.*, Alessandro Acquisti, Curtis Taylor & Liad Wagman, *The Economics of Privacy*, 54 J. ECON. LITERATURE 442, 469 (2016) (summarizing the scholarship of Amalia R. Miller & Catherine E. Tucker).

whether to allow the FTC authority to assert exclusive jurisdiction when necessary, to ensure consistent and coherent application of federal law.

Second, data collection and use are endemic to our economy and are the engines of significant economic growth and consumer benefit. Any federal privacy bill will thus apply to a vast array of companies, large and small. A private right of action will have a substantial and unwarranted negative impact, particularly on small, innovative, businesses, deterring them from innovating and growing jobs, as they prioritize lawsuit avoidance over doing what they do best. Any new federal privacy law must provide for rules and regulation, but it should do so in a way that best permits for future growth and innovation and that encourages investment and risk-taking. Government enforcement of a privacy law, rather private lawsuits, is the best way to balance those interests.

My remarks today highlight the work ahead of us on privacy legislation and I realize that it will be difficult and challenging. However, these are decisions that we must get right – there is so much at stake.

Thank you very much for your time today and I look forward to taking any questions you may have.