UNITED STATES OF AMERICA

Federal Trade Commission

Opening Keynote of Commissioner Noah Joshua Phillips

Future of Privacy Forum:
9th Annual Privacy Papers for Policymakers

Washington, DC
February 6, 2019

Thank you, Mary, for the kind introduction; and thanks to the Future of Privacy Forum for sponsoring this event. The work that FPF fosters – the work that all the privacy scholars in the room do every day – is as important now as it has ever been.

Before I explain why, the obligatory caveat: I'm speaking this evening for myself, not for the Federal Trade Commission or my fellow Commissioners.

Ours is a watershed moment for consumer privacy in America. Data sharing and use are endemic to modern commerce and now hold our collective attention.

- On an almost daily basis, we read press reports on new consumer privacy issues.
- Policy-makers around the world are training their focus on privacy. Congress is holding hearings; the Administration is inviting comment; states are legislating; Europe has not only adopted the General Data Protection Regulation but is pushing other countries to follow suit.

- While I won't opine on the actual chances for federal legislation, both Republican and Democratic lawmakers report that new consumer privacy legislation may move forward in 2019.

The privacy conversation has gone public. In many ways, that is good. Increased awareness can help inculcate a culture of 'privacy be design' in industry;[1] it can foster the digital ethics on which the ICDPPC focused in October in Brussels. Awareness can help serve what many view as a market failure of consumer information about what happens with data consumers generate.

But the *sturm und drang* of our public conversation about privacy – often regrettably including fear-mongering stoked by ambition of one kind or another – too often drowns out the rigor, thoughtfulness, and nuance that good policymaking requires.

To borrow a phrase from Professor Lilian Edwards and Michael Veale's paper, it often feels that, amid all the privacy noise, "any remedy in a storm has looked attractive."[2]

That's panic, not policy.

We – the community of academics, policymakers, and law enforcers who focus on privacy – need to resist that impulse.

To develop policy on the future of consumer privacy, or should I say to develop *good* policy on the future of consumer privacy, we must strive to know and understand more.

---

[1] *See, e.g.,* Ari Ezra Waldman, *Designing Without Privacy*, 55 HOUSTON L. REV. 659, 713 (2018).
[2] Lilian Edwards & Michael Veale, *Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For*, 16 DUKE L. & TECH. REV. 18, 18 (2017).

We should be empirical and thoughtful.

We should make conscious and informed choices based on what we learn, not what we presume.

We should be honest in when we are making normative judgements and how they work as applied.

Or, as Jef Ausloos and Pierre Dewitte recognize in the context of their empirical research, we need to "have an informed debate – grounded in practical reality".[3]

Let me cite just a few examples where I fear much of the policy discussion isn't meeting this standard.

First, what problem – or problems – are we solving? Last November, I testified before the Senate Commerce Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security. Privacy is a nebulous term, meaning different things to different people. So I urged the senators first to agree on the harms they wished to address – then to fashion solutions.

- Physical injury and financial loss?
- A type of emotional distress?
- A sense of surveillance or creepiness?

Professor Citron's article, "Sexual Privacy,"[4] is an excellent example of a series of privacy harms with a distinct impact. Reasonable minds can and do differ on which harms we need to remedy in privacy legislation. But, without frank

[3] Jef Ausloos & Pierre Dewitte, *Shattering One-Way Mirrors. Data Subject Access Rights in Practice*, 8 INT'L DATA PRIVACY L. 4, 4 (2018).
[4] Danielle Keats Citron, *Sexual Privacy*, YALE L. J. (forthcoming 2019).

discussion and consensus on the ends, there is no way to developing appropriate means, and we are almost guaranteed to miss the mark.

Another example involves the collateral consequences of new legislation. I'm fairly confident that the drafters of the GDPR did not desire to entrench Google and Facebook in the ad-tech market, or to reduce investment in European technology firms. But, at least from some initial reports,[5] that may be what is happening.

Do we want U.S. legislation that will similarly impede innovation and competition in pursuit of enhanced consumer privacy?

The right balance of those priorities is a value judgement, and some reduction in competition may be worth it. But, using expertise and data, we should do our best carefully to plot out and consider the real-world consequences of any new regulation, tweaking the balance and making educated choices among sometimes competing priorities.

A third brief example. Data portability is a frequent theme in privacy regulation. Some people think of it as an outcome that will empower consumers *and* foster competition. How has it worked in prior legislation? HIPAA – the Health Insurance Portability and Accountability Act – is worth a serious look. But one hears little about our experience with HIPAA in the current debate. Here is our chance to learn about data portability in the wild – the pros and cons, the pitfalls

[5] 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; 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.

and impact. We should be analyzing and using that experience to engage in an informed discussion.

These questions and countless others is where the work supported and encouraged by FPF comes in. The name of this event really says it all – Privacy Papers for *Policymakers*. Not academic research of interest to a limited audience – not that there is anything wrong with the unadulterated search for truth – but the type of analysis that should inform policy decision-making, that should inform Congress as it wrestles with consumer privacy.

Edwards and Veale's paper, "Slave to the Algorithm," is a helpful reminder of the need to match remedies to problems. They conclude that, practically, the 'right to an explanation' is unlikely to address concerns about algorithmic decision-making. New rules should solve the problems identified and avoid providing unproductive, or even counterproductive, new rights.[6]

Do the FTC's existing tools – the Fair Credit Reporting Act and Equal Credit Opportunity Act in particular – provide sufficient protection against algorithmic unfairness, and, if not, why not? In a recent case, RealPage, the FTC entered into a settlement for three million dollars with a tenant screening company whose automated screening software, allegedly, associated consumers seeking apartments with criminal records that did not belong to them.[7]

---

[6] Edwards & Veale, *supra* note 2, at 81.

[7] *See* FTC Press Release, *Texas Company Will Pay $3 million to Settle FTC Charges That it Failed to Meet Accuracy Requirements for its Tenant Screening Reports* (Oct. 16, 2018), https://www.ftc.gov/news-events/press-releases/2018/10/texas-company-will-pay-3-million-settle-ftc-charges-it-failed.

The broader point is that privacy regulation is a complex policy question and we need to test solutions – whether on algorithmic unfairness or portability or what have you – as best we can before they are implemented, lest they create burdens without benefits, or, worse, the false perceptions of protection.

I've long felt that the current U.S. privacy scheme gets a bad rap.[8] Though critics contend the U.S. has no federal privacy law, in fact we have been doing privacy at the federal level for over 40 years, with a risk-based scheme focusing regulation and enforcement on the areas of greatest potential consumer harm. We've done this while fostering tremendous innovation and economic growth.

Still, I do think that the present process of Congress evaluating our data security and privacy laws is extremely valuable. Perhaps we will target another case of heightened risk, as Professor Citron's paper lays out. Maybe Congress will take a comprehensive approach. Again, such an approach requires a clear view of the goals, not just the tools. It is not enough to say we need penalties. Or rulemaking authority. Those are tools, and they only make sense if built and used properly. And they come with costs, deterrence of efficient conduct, or the empowerment of unelected bureaucrats – like me.

All of this is to say that if the U.S. is going continue to protect privacy and foster innovation and growth, our policy should be grounded in facts and analysis, not speculation, hope, or panic.

---

[8] *See* Noah Joshua Phillips, Commissioner, Federal Trade Commission, Remarks at the U.S. Chamber of Commerce and the American Chamber of Commerce to the European Union: *Our American Privacy* (Oct. 23, 2018), https://www.ftc.gov/public-statements/2018/10/our-american-privacy.

We must be careful, smart, and informed.

We must understand the problems we are trying to solve and how the solutions match up in practice.

We must be honest and cognizant of tradeoffs, and not succumb to the "Nirvana fallacy".

We must ask the right questions and do the hard work, not settling for simple answers.

If we do this, and only if we do this, we may be able to craft a revised privacy regime that has legitimacy and efficacy both at home and abroad. That is why your work is so important. So thanks, to FPF; to the scholars we are honoring this evening; to all of you.