United States of America
FEDERAL TRADE COMMISSION
WASHINGTON, DC 20580

Remarks of Commissioner Rebecca Kelly Slaughter[1]
FTC Hearing #12
The FTC's Approach to Consumer Privacy

April 10, 2019

Good afternoon and welcome back to the last half of our two-day hearing focusing on the FTC's approach to consumer privacy. I'm Rebecca Kelly Slaughter. I have had the pleasure of listening to and learning from each of our 11 hearings to date, but this one I must admit I have enjoyed the most, and has been one of our most important. I want to thank all of the esteemed panelists who have shared their insights, and I also want to thank our Office of Policy and Planning for their tireless work on these hearings and BCP's Division of Privacy and Identity Protection for their leadership in planning this event, in particular Elisa Jillson, Jim Trilling and Jared Ho.

I'd like to use my time today to speak briefly about three aspects of the FTC's approach to consumer privacy that I see—or hope to see—evolving: the role of notice and choice, the integration of competition and consumer protection concerns, and FTC authority and resources.

The Limitations of Notice and Consent: I had no choice and did not really agree.

The notice and consent framework began as a sensible application of basic consumer protection principles to privacy—tell consumers what you are doing with their data and secure their consent. But in order for a notice and consent regime to be effective, both elements must be meaningful—notice must give consumers information they need and can understand, and consumers must have a choice about whether to consent. I am concerned that today, when it comes to our digital lives, neither notice nor consent is meaningful.

By now we've all heard the estimate that it would take 76 working days to read all of the privacy policies one encounters in a year.[2] It is no wonder then that a more recent study from 2016 demonstrated that 98 percent of potential users of a social media site had no problem clicking "I agree" to privacy policies and terms of service that disclosed sharing with the NSA

[1] The views expressed in these remarks are my own and do not necessarily reflect the views of the Federal Trade Commission or any other Commissioner.
[2] Madrigal, Alexis C. "Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days." *The Atlantic*, Mar. 1, 2012, https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/.

and paying for the service by signing away your first-born child.[3] As an oldest child and as a parent, I have to assume that this was a close reading failure and not an indictment of the "strong and spirited" dispositions of so many first-borns.

Another study showed that a majority of Americans believe that when a company merely posts a privacy policy, it means that the company does not share user data.[4]

These studies and myriad others simply validate what we all already know: clicking through these policies presents little value to consumers. They are often long and confusing, and even when they try to be more succinct, their sheer number places an insurmountable burden on consumers trying to navigate the marketplace. I'm not saying that privacy policies don't have value—they do. At their best, they force companies to think through how they are treating consumer data and publicize that promise. This is beneficial to the company, to researchers, and to law enforcement, but it provides little immediate benefit to the consumer trying to access the services she needs while maintaining some control over their privacy.

Furthermore, as we heard several commenters note over the last two days, we cannot consider click-through consent to present a meaningful choice. The "choice" is illusory because even if a consumer could read and understand the notice, she often has no choice but to consent in order to reach a digital service that has become necessary for participation in contemporary society. And, as the panelists discussed yesterday, even where it appears consumers have given valid consent, that agreement might be a product of manipulative dark patterns.

It is easy to decry the limitations of the notice and consent framework and far harder to reach a conclusion about what should replace it. We could adopt the GDPR approach of trying to cure the problem by presenting more useful information to consumers, more plainly. The jury is still out on its effectiveness, but no doubt improved notice and consent over specific practices could and should be debated as part of a U.S. privacy framework going forward. We could also look to the CCPA's requirements to present consumers with meaningful opt-out choices, particularly over the sale or transfer of their data. Or we could impose more concrete purpose limitations, where data can only be used by a company for the purpose for which it was provided. The rich debate on this topic this morning demonstrates that there are a number of paths to improve the current framework.

In the midst of this debate, I want to put my thumb on the scale for solutions that do **not** place all or even most of the burden on the consumer. It is the job of the entity collecting, transferring or using the data to accurately and fairly assess consumers' expectations about how their data will be used, and to meet those expectations. If the company misuses the data, law enforcement needs to be able to step in to hold companies accountable. I also want to advocate for solutions that deliver consumers meaningful choices, which requires policyholders to consider both consumer protection and competition concerns.

---

[3] Obar, Jonathan A. and Oeldorf-Hirsch, Anne. "The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services." *TPRC 44: The 44th Research Conference on Communication, Information and Internet Policy,* Apr. 2, 2016, https://ssrn.com/abstract=2757465.

[4] Smith, Aaron. "What Internet Users Know About Technology and the Web." *Pew Research Center Internet & Technology*, Nov. 25, 2014, https://www.pewinternet.org/2014/11/25/web-iq/.

Data Privacy: Bringing Competition and Consumer Protection Together.

The FTC is lucky to have both competition experts and consumer protection experts working together in one agency. Many of these hearings have underscored how intertwined traditional consumer protection concerns are with competition concerns, particularly in the area of data privacy. The limitations of the notice and consent framework is one such area that raises both concerns. We'd all rather a world where digital platforms compete for users on metrics such as privacy. But today consumers often need to cede all control over their data to participate in or use certain services that have become critical to their everyday lives; they don't have the option to turn to a competing, more privacy-protective service. This dearth of real choice is a privacy problem, but it is also a competition problem.

Lack of choice is not the only area where privacy and competition concerns collide. The increased risks to consumers arising from consolidated pools of data also raise competition and privacy concerns. In today's economy, when two firms combine they are almost certainly marrying large amounts of personal data as well. Does the emerging firm have the ability to manage that data or related technology safely? Did consumers expect when they shared data with company A that one day it might be combined with data shared with company B? And will the emerging firm use the combined data in a manner that is consistent with consumers' original expectations?

And perhaps most obviously, developing a national privacy framework necessitates balancing competition and privacy goals. We must take care that in attempting to secure increased protection for consumer data privacy we don't inadvertently further entrench incumbents or otherwise hinder competition and choice. This is a concern that has been expressed frequently by those who oppose new privacy laws. I agree it is a concern, but I do not agree that it means we should stick with the status quo, which neither protects privacy nor provides competition.

As these hearings demonstrate, the FTC is already moving toward more blended debates and dialogues about these issues. I am particularly optimistic that this trajectory will continue through the Chairman's new technology task force, which will leverage both our antitrust and privacy expertise.[5]

Authority and Resources: We Need More.

I want to conclude today by spending a minute on the FTC's authority and resources devoted to consumer privacy. One of the questions posed to ground this hearing is what should the role of the Commission be in the privacy area? The FTC serves many roles in this area: business counselor, consumer educator, researcher, and advocate—but our most critical role is that of enforcer. Thoughtful policy debates and balanced legislation will be to no avail if the resulting statutory framework does not provide for serious enforcement mechanisms and resources to incentivize compliance.

Today the FTC's privacy enforcement centers around a handful of sector specific rules—FCRA, COPPA, Safeguards—and our Section 5 unfairness and deception authority. Our rules

[5] Press Release, "FTC's Bureau of Competition Launches Task Force to Monitor Technology Markets," Feb. 26, 2019, https://www.ftc.gov/news-events/press-releases/2019/02/ftcs-bureau-competition-launches-task-force-monitor-technology.

allow us to protect children's information online and to help ensure that non-bank financial institutions and the CRAs are protecting consumer data, but they leave some gaping holes. Large categories of personal data are not covered by our rules: what we share on social media, what we share with many retailers, including our largest online retailers, and what we share with apps and devices, even when we share personal health or relationship information. And that is just the data that we intend to share. When our data is harvested and collected without our knowledge or expectation? In most cases, our rules don't cover these practices either. Even when we do have specific rules in place, that does not guarantee that we have penalty authority—for COPPA and FCRA we do, but we have no penalty authority under the Safeguards Rule.

In order to protect consumers' data and privacy beyond the narrow fields covered by our rules, we must rely on our Section 5 unfairness and deception authority. The FTC has been nimble and aggressive in its attempts to use this hundred year-old statute to police today's technology-driven marketplace—with many successes. But we face real limitations proceeding under Section 5. We cannot seek monetary penalties for data security and privacy violations in the first instance and generally quantifying consumer injury in terms of dollar amounts is challenging. Moreover, without specific statutes or rules defining practices in this area, both courts and companies have been left with questions about whether particular behavior is prohibited.

Because of these limitations, the majority of the Commission supports the enactment of a comprehensive federal privacy law that does three things in terms of enforcement: (1) empowers the FTC to seek significant monetary penalties for privacy violations in the first instance; (2) gives the FTC APA rulemaking authority, to allow us to craft flexible rules that reflect stakeholder input and can be periodically updated to keep up with technological developments; and (3) repeals the common-carrier and nonprofit exemptions under the FTC Act to ensure that more of the entities entrusted with consumer data are held to a consistent standard.

But the single biggest change that would help the FTC in its role of enforcer of data privacy laws right now, would be an increase to our resources. We currently have about 40 full-time employees devoted to privacy and data security. We have five full-time technologists, most of whom serve all of our consumer protection missions, not just data privacy. The U.K. Information Commissioner's Office by contrast has 500 employees. The Irish Data Protection Commissioner has over 100. We have a much larger jurisdiction and much blunter tools than our European colleagues, yet we have a fraction of the personnel.

The FTC's current annual budget is $306 million and, like most organizations, our greatest expense is also our greatest resource: staff. Approximately two-thirds of our current budget is allocated to pay and benefits for staff. If the FTC received an additional $50 million in ongoing annual funding, we could hire approximately 160 more staffers. An additional $75 million would enable us to bring onboard 260 more staffers. That would, incidentally, put us around the staffing level we had in 1982—before the internet—and still well below the levels in the late 1970s.

With increased staff, the FTC would be able to devote more resources to enforcing our existing rules and any future privacy rules. We would also be able to expand the number of staff dedicated to conducting compliance reviews of our privacy and data security orders. We would also be able to do more than just react to the worst behaviors in the marketplace; additional

staffing could be used to generate original research, conduct 6(b) studies of industry and, of course, focus on strategic targeting, investigation, and case generation.

The threats to privacy that consumers face in the marketplace are growing and grow ever more complicated. Our budget has not kept pace with these developments, and our future as an effective enforcer in the area of data privacy hinges on an expansion of both our authority and our resources. I thank you again for letting me participate in today's hearing and look forward to hearing more on this topic from our experts this afternoon discussing their views on the adequacy of the FTC's toolkit.