STATEMENT OF

CHAD A. MARLOW
SENIOR ADVOCACY AND POLICY COUNSEL
AMERICAN CIVIL LIBERTIES UNION

For a Hearing on

"Data Ownership: Exploring Implications for Data Privacy Rights and Data Valuation"

Before the

United States Senate
Committee on Banking, Housing, and Urban Affairs

Thursday, October 24, 2019

For further information, please contact Chad A. Marlow, Senior Advocacy and Policy Counsel, at cmarlow@aclu.org.

Chairman Crapo, Ranking Member Brown, and Members of the Committee on Banking, Housing, and Urban Affairs, on behalf of the American Civil Liberties Union (ACLU)[1], I want to thank you for the privilege of testifying before your Committee today.

The ACLU is strongly concerned about the data as property model and how it is being presented to the American public and its lawmakers. While the data as property model may have merit as a tool for redistributing the money that is currently being made off the sale of personal information, any claim that it advances privacy is false. To the extent Congress is seeking to provide greater private protections for Americans' personal information, what we need is an affirmative consent-based model that provides all individuals the ability to opt-in (or not) to the sharing of their personal data. Whether consenting to such use results in monetary gain is a separate matter, and does not in and of itself advance privacy. We should not countenance misleading assertions that the data as property model is itself pro-privacy.[2]

A central tenet of the data as property model is that the government should establish – through regulating and policing a universal marketplace of personal data – that individuals are "owners" of their personal information and, consequently, have a property-based right to sell or refuse the sale of their data to third parties. However, if the objective is privacy protection, policymakers have identified other approaches that more directly facilitate advancements in the cause of personal information privacy and do not carry the adverse privacy risks associated with the data as property approach. For example, two state laws passed last year[3] – the "California Consumer Privacy Act",[4] which allows consumers to opt-out of their personal information being sold, and Maine's "Act To Protect the Privacy of Online Customer Information",[5] which takes the superior approach of not allowing a person's information to be sold without first securing their "opt in" permission – made important advances in protecting individual privacy, without treating data as property or focusing on its monetary value. Rather, they advanced privacy by empowering individuals to exercise control over their personal information. Indeed, at a time when our existing laws at the federal level and in most states are wholly insufficient to ensure that

---

[1] For nearly 100 years, the ACLU has been our nation's guardian of liberty, working in courts, legislatures, and communities to defend and preserve the individual rights and liberties that the Constitution and laws of the United States guarantee everyone in this country. With more than eight million members, activists, and supporters, the ACLU is a nationwide organization that fights tirelessly in all 50 states, Puerto Rico and Washington, D.C., to preserve American democracy and an open government.

[2] Chad Marlow, *Beware the Tech Industry's Latest Privacy Trojan Horse*, ACLU (Mar. 18, 2019) https://www.aclu.org/blog/privacy-technology/medical-and-genetic-privacy/beware-tech-industrys-latest-privacy-trojan.

[3] Françoise Gilbert, *Maine Follows California Lead: Prohibits ISP Use, Sale, Disclosure of Online Consumer Information Without Prior Affirmative Consent*, The National Law Review (June 10, 2019) https://www.natlawreview.com/article/maine-follows-california-lead-prohibits-isp-use-sale-disclosure-online-consumer.

[4] SB-1121, 2017-2018 Leg., (Cal. 2018) *also available at* https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121.

[5] S.P. 275, 2019 Leg., 129th Sess. (Me. 2019) *also available at* http://www.mainelegislature.org/legis/bills/getPDF.asp?paper=SP0275&item=1&snum=129.

individuals have control over protecting their personal information, the data as property model simply distracts us from pursuing meaningful privacy legislation.

Four aspects of the data as property model – which essentially mandates the creation of a government regulated and policed marketplace for personal information—would be especially harmful to privacy and free speech:

Creating Conflict at the Time Individuals Might Otherwise Choose to Protect Their Personal Information

To understand why the data as property model is concerning, one should start by looking to how it would be effectuated. Namely, at the time a person's information is collected – which is when pro-privacy laws typically mandate the disclosure of one's data privacy rights – a government mandate would require the simultaneous advertising of the individual's ability to surrender their privacy by selling their personal information. To make the decision to sell one's data seamless, where this model has been pushed by data sales facilitators on the state level, the bills further require data sales authorization forms be concurrently provided.

Imagine, as was the focus of a data as property bill in Oregon earlier this year, how uncomfortable that exchange might be where, in the course of ongoing medical treatment, a doctor requests a patient provide consent so they can sell the patient's personal information. Now further imagine what pressure might be applied where the doctor has been incentivized to secure consent by being offered a cut of the sale revenue for the data.

Instead of giving consumers meaningful control over their personal information, many of the private sector entrepreneurs who are advocating for the data as property model want to use the power of the government to mandate that the marketplace for selling data – one they will very profitably help to facilitate – is advertised to all persons at the time their information is collected. We have seen this as a central feature of the data as property bills being introduced in states, like the previously referenced bill in Oregon,[6] where as soon as the bill was understood to be a privacy Trojan Horse, it was soundly rejected. In fact, no data as property bill has been adopted in any of the states in which they have been pursued or introduced, which includes Oregon, Maryland, Hawaii, California, Washington, Montana, Arizona, Georgia, New Jersey, Massachusetts, and Pennsylvania.

If anything, when it comes to privacy, what the data as property model actually does is create a hedge against the growing likelihood that Congress and the states will pass tougher privacy laws. Specifically, it would ensure that, should stronger privacy protections be implemented, the data sales marketplace – which relies upon convincing people to relinquish their privacy – will be advertised right alongside any required notifications about individuals' new privacy rights. As

[6] S.B. 703, 2019 Leg., 80th Sess. (Or. 2019) https://olis.leg.state.or.us/liz/2019R1/Downloads/MeasureDocument/SB703/Introduced.

Congress explores how to better protect Americans' privacy, it should strongly resist supporting the data as property model, which would undermine those efforts to directly protect privacy.

Widening of Digital Divide and Disproportionate Harm to the Most Vulnerable Individuals

The high value Americans place on their privacy is universal[7] and nonpartisan.[8] It is wisely enshrined in our Bill of Rights.[9] As a result, adopting a model where persons with less wealth are likely to end up with less privacy should give lawmakers pause.

Americans who are economically secure will find it easy to reject offers to surrender their private information in order to make a few extra dollars. But that might not be the case for an elderly person who has a hard time affording their prescriptions and rent. It may be too tempting a sales pitch for a family that is struggling to put food on their table. For persons who live in rural areas, where the cost of online access may already be steep, a chance to offset those costs while online may feel impossible to turn down. And so they will agree, when pressed, to sell their private information for an unquantified amount of money.

As a consequence, a government endorsed data as property model would only serve to further expand this country's existing digital divide[10], where persons already enduring socioeconomic or regional economic disadvantages – including disproportionately, persons of color – frequently have little or no choice but to rely on cheaper, non-encrypted cell phones, free email, and other more affordable but less secure tech products. The digital divide is a privacy divide, and the data as property model would only serve to worsen it.

Requirement of a Universal Unique Tracking Identifier for All Persons

One of the most pernicious practical requirements of any data as property model would be the need to create some form of universal unique tracking identifier for all personal information. To track who owns personal data, who has sold it, who must pay, and who gets paid, each piece of data must be tagged with some form of a universal identifier.

There likely would be no opt-out from a universal unique tracking identifier for anyone, even for those who consistently refuse to sell their personal information. Why? Because legal compliance is likely to not only require companies to identify what data they are permitted to sell and resell, but also to identify unlawfully distributed data as to which sales permission has been denied.

---

[7] NATIONAL SCIENCE BOARD, AMERICANS' ATTITUDES TOWARD INFORMATION PRIVACY IN THE WORLD OF BIG DATA at 1, *also available at* https://nsf.gov/statistics/2018/nsb20181/assets/404/americans-attitudes-toward-information-privacy-in-the-world-of-big-data.pdf.

[8] Carl M. Cannon, *Digital Privacy, a Non-Partisan Issue*, Real Clear Politics (July 23, 2013) https://www.realclearpolitics.com/articles/2013/07/23/digital_privacy_a_non-partisan_issue_119332.html.

[9] U.S. Const. amend. IV.

[10] Gry Hasselbach and Pernille Tranberg, *Privacy is creating a new digital divide between the rich and poor*, The Daily Dot (Oct. 23, 2016) https://www.dailydot.com/layer8/online-privacy-data-ethics/.

The need for a universal unique tracking identifier gets particularly apparent, as well as difficult to implement as the lines blur on who owns what data. What happens when data is sold that has information about multiple parties, like DNA or a group photo? Does everyone have to agree and get paid? What happens when some parties whose personal information is contained is data elected to sell it and others refuse? Who prevails?

In the end, whether people choose to sell their personal information or not, the effectuation of the data as property model, including the universal unique tracking identifier it may require be attached to all personal data, raises significant privacy concerns.

Harm to Free Speech on the Internet

The need to track all communicated personal information, in order to effectuate and enforce the data as property model, will have an adverse impact on free speech. For example, every time a person shares content on the internet, sends an email or text message over a public network or using a free application, or posts a picture of themselves or their family or friends on social media, personal information about them will be transmitted, either within the communication itself or in its accompanying metadata. As a result, under the data as property model, it will need to be tracked and associated with the person who communicated it using a universal unique tracking identifier. Once the public becomes aware of this fact – and if the ACLU doesn't warn them, one of dozens of other privacy organizations certainly will – the public will know it has lost the ability to communicate anonymously.

This would have an adverse effect on the free exchange of ideas, including on the ability to communicate private thoughts, or messages intended for a limited audience, or ideas that are either unpopular or represent opinions one is exploring but does not necessarily endorse. Privacy and free speech frequently go hand in hand, and that is certainly the case with the harms presented to them by the data as property model.

A Better Way: Adopt Meaningful Privacy Legislation

If Congress wants to pass a law that creates meaningful privacy protections for Americans - if Congress wants to pass a law so that every time Americans use the internet, or social media, or complete a commercial transaction, they do not have their personal information gathered and offered up for sale to third parties – it does not need to treat data as property to do so. In fact, passing legislation that treats data as property carries specific harms that would undermine that goal.

The government should not be promoting privacy as a resource to be bought and sold. A growing number of state constitutions[11] now recognize that privacy is a fundamental right, including the constitutions of the home states of this Committee's members from Arizona, Hawaii, Louisiana, Montana, and South Carolina, along with many others.

The proper response to the pervasive loss of individual privacy is to pass stronger privacy laws,[12] not just to throw up our hands and conclude the only issue left to tackle is who gets the money when people's data is sold. Yes, privacy protections for personal information are weak in this country, but Congress and the states have the ability to strengthen them. And they should. Limiting data collection, retention, and further transfers without a person's clear, distinct, and informed permission is a strong place to start.

Additionally, companies should be prohibited from denying a good or service to someone who chooses to exercise their privacy rights, and consumers should have a private right of action to seek compensation when their privacy rights are violated. Most relevant to today's discussion, we should not be looking to a data as property model, which monetarily incentivizes people to give up their privacy, to enhance privacy protections.

Again, if those who support the data as property model want to talk about it as a potential way to create a more robust and equitable marketplace for the sale of personal data, by all means they should make that argument, but they need to stop advancing the false narrative that the data as property model is pro-privacy.

Congress has the ability to adopt laws that truly empower Americans to better protect their personal information without undermining privacy in the process, and I have confidence that you will.

Thank you again for the opportunity to testify today. I look forward to answering your questions.

---

[11] Privacy Protections in State Constitutions, National Conference of State Legislatures (Nov. 7, 2018) http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx.

[12] *Consumer Perspectives: Policy Principles for a Federal Data Privacy Framework Before the S. Comm. On Commerce, Science, and Transportation*, 116th Cong. 3 (2019) (statement of Neema Singh Guliani, Senior Legislative Counsel, ACLU) *also available at* https://www.commerce.senate.gov/services/files/79ABFD7A-8BEB-45B5-806A-60A3467255DD.