Supplemental Testimony before the Senate Judiciary Committee
On the General Data Protection Regulation and California Consumer Privacy Act: Opt-ins, Consumer Control, and the Impact on Competition and Innovation

Roslyn Layton
Visiting Scholar

April 10, 2019

Chairman Graham, Ranking Member Feinstein, and Members of the Committee, thank you for the opportunity to provide additional testimony for the record. Please find my answers to your questions. Please find some additional articles for the record in which I address issues such as the model and costs of privacy regulation.

The costs of California's online privacy rules far exceed the benefits

Roslyn Layton | March 22, 2019 | AEIdeas
http://www.aei.org/publication/the-costs-of-californias-online-privacy-rules-far-exceed-the-benefits/

Cost-benefit analysis (CBA), while imperfect, improves policymaking. However, CBA is frequently performed after the fact to justify regulatory decisions already made. Some reject CBA outright, saying that costs and benefits are too difficult to quantify, or because its conclusions do not support predetermined policy preferences. To overcome quantitative and cognitive difficulties, economists propose "back of the envelope" CBAs, ensuring that analysis is done *before* rulemaking and incorporates observed values policymakers can understand. George Washington University's Daniel Pérez recently presented a preliminary CBA in light of privacy regulation from Europe and California.

Benefits of privacy regulation

Pérez attempted to find the best case for regulation. He assumed one in four mobile users would take advantage of privacy regulation based on reported willingness to pay (WTP) for the privacy of personally identifiable information using techniques for concealing browser history and geolocation data and for the ability to access, correct, and transfer personal data. His model for mobile apps accessed by Android users in the US builds on frameworks developed by Hann et al. (2007), Savage and Waldman(2013), Acquisti et al. (2013), and Fuller (2019). The benefits are calculated by WTP for a typical privacy configured app ($3.47), the average number of apps per user (23), the lump sum WTP for privacy functionality ($13.77), and the number of

smartphone users willing to pay for such services (generously estimated to be 25 percent of 257,300,000 smartphone users). Importantly, apps are downloaded in year one with updates in future years. This calculation yields an upfront benefit of $8.6 billion and $6.1 billion in the following years. With discounting, the accumulated benefit is between $48 and 56 billion in a decade.

These benefits seem small, especially relative to the $1.6 trillion digital economy, but the numbers are not out of line with other studies of discrete privacy rights from Europe's General Data Protection Regulation (GDPR). Indeed, studies of users' willingness to pay for an ad-free Facebook suggest similar amounts. Forty-two percent of respondents said they would pay up to $5 per month, a quarter would pay up to $10, and one-third would pay $11 or more). These numbers correspond to Facebook's average revenue per user per month of $11 in Q4 2018, the value that Facebook earns on advertising and other services divided by the number of users. This figure presumably includes the "risk" people undertake to use Facebook. Despite many policymakers' doomsday scenarios following the Cambridge Analytica scandal and the 2016 election, Facebook's revenue and usage has increased in all geographies in the past two and a half years.

Costs of privacy regulation

While Pérez generously estimates the benefits of privacy regulation, he conservatively estimates the costs at $24.5 billion for upfront compliance and lost advertising revenue. The present value of the annualized costs are $57 – $63 billion in the coming decade. When balanced against the benefits, the outcome is a total loss of $7 – $8 billion.

If the actual costs from the GDPR are any indication, the real costs of the California Consumer Privacy Act (CCPA) are likely to be much higher. Six months after the implementation of the GDPR, 41 percent of firms surveyed by Verasec reported that compliance cost had exceeded their budgets.

We also can examine the compliance costs already being borne by California firms preparing for the CCPA. TrustArc commissioned a survey of the readiness of 250 firms serving California from a range of industries and company size in February 2019. It reports that 71 percent of the respondents expect to spend at least six figures in CCPA-related privacy compliance expenses in 2019 — and 19 percent expect to spend over $1 million. Notably, if CCPA were in effect today, 86 percent of firms would not be ready. An estimated half a million firms are liable under the CCPA, most of which are small- to medium-sized businesses. If all eligible firms paid only $100,000, the upfront cost would already be $50 billion. This is in addition to lost advertising revenue, which could total as much as $60 billion annually.

Conclusions

Conservatively, costs of privacy regulation exceed benefits by four fold. Some claim that benefits could increase because of fines and lawsuits. While this could be true, the substantive fines would come from only a few firms that could be prosecuted under existing laws and consent decrees. In any case, payouts wouldn't be realized for years due to the litigation sure to ensue. In the meantime, all firms would have to bear increased costs, and many would exit, leaving larger firms greater market shares, as already experienced with the GDPR.

Because people don't pay out of pocket for most apps today and already have the option to turn off tracking, it remains to be seen if even modest benefits of $6 – $9 billion annually are realized. Under the California framework, users inevitably will have fewer apps to choose from as the long tail of advertising-supported apps will be cut. Pérez suggests a radical idea that privacy legislation should be based on evidence that regulation will actually advance privacy outcomes in ways that consumers value. The lion's share of the money generated by the regulation flows to software upgrades, privacy consultants, and lawyers — not consumers. An upcoming Senate hearing on "Small Business Perspectives on a Federal Data Privacy Framework" is likely to provide additional information for this discussion.

Should online privacy legislation be based on trust or control?

Roslyn Layton | April 8, 2019 | AEIdeas
http://www.aei.org/publication/should-online-privacy-legislation-be-based-on-trust-or-control/

Peter Winn, director of the Office of Privacy and Civil Liberties and acting chief privacy officer at the Department of Justice spoke at AEI last week. He noted that trust is fundamental to the efficacy of any institution, whether a firm, a country, or the DOJ itself. He described the DOJ's duty to "enforce the law, defend the interest of the United States according to the law, and to ensure fair and impartial administration of justice. . . . That's the value we create, and our brand has to be trusted." Winn's office is responsible for the DOJ's adherence to many privacy and data protection laws including the 1974 Privacy Act, among the world's first laws regulating government use of computerized information. The act itself does not guarantee a right of privacy, but rather ensures the mutual interest and partnership of individuals and government to maintain accuracy of information.

Leviathan state, property rights, or multi-stakeholder governance?

Winn noted the false choice that online privacy governance must either be a leviathan state (social control with an absolute sovereign) or a free-market system based purely on property rights. He highlighted the work of Nobel economist Elinor Ostrom on common pool resources as a trust-based alternative and noted how such a model is already used in the Federal Information Processing Standards, or FIPS, and the FBI Domestic Investigations and Operations Guide, the set of standard operating procedures informed by the experience of FBI agents.

For illustration, Winn described the "blabbermouth system," which schoolyard children use to keep each other honest through trust and graduated system for punishments. While the teacher is on hand to intervene in serious situations, if she intervenes too much, trust among the children breaks down, and they start to game the teacher. The blabbermouth system allows

the children to learn, practice good behavior, and keep compliance costs low. “When users are genuinely engaged in decisions regarding rules affecting their use, the likelihood of them following the rules and monitoring others is much greater than when an authority simply imposes rules,” notes Ostrom. Such multi-stakeholder governance has been the norm for the internet itself, standard-setting organizations, and other areas of emergent science and technology in which knowledge about the future is limited.

The US risk-based model versus the EU’s command and control model

The US has over time implemented many rules to protect individuals’ information from overreach by the administrative state while recognizing the benefits of some information being in the public domain (for example, phone numbers and addresses in telephone books, subject to opt out for a fee). Hence, policy has generally promoted the importance of trust, a confidence in the reliability of a system, rather than the absolute right of an individual to seclude information about oneself.

Over time a system to analyze risk emerged, and, recognizing the sensitivity of certain information, rules were adopted to manage sensitive data, notably that of children, health, and finance. Meanwhile other sectors and industries remain subject to discipline based on actual harms and tests for unfairness and deception. Notably, this framework of permissionless innovation has been important for consumers and entrepreneurs.

The European Union’s General Data Protection Regulation is predicated on information being finite and extinguishable, hence the demand of a right to erase it or retire it at the end of its life. Its underpinnings can be traced to privacy laws in West Germany that were adopted in response to the horrific surveillance conducted by the Stasi, the East German secret police.

Given its experience with two devastating world wars, Europeans can be understandably pessimistic about the future and take a negative view of how personal information can be abused.

The US, on the other hand, having the longest-lived constitutional democracy and the good fortune of two relatively peaceful neighbors, has a relatively optimistic view of the future.

The right to know versus the right of privacy

Winn noted that knowledge about people is what businesses use to create economic value for customers, and it's what law enforcement agencies use to ensure public safety. He contrasted the benefits of America's historical risk-based model for online data with the GDPR's command and control model and its universal rules for all contexts, which has created negative consequences that go far beyond their intended purposes.

For example, since the GDPR's implementation, the contact information of domain registrars published in the WHOIS online database is no longer available. This frustrates the DOJ's ability to carry out its mission to detect and deter cyberthreats from malicious online actors, who previously could be discerned from now-obscured public information. Indeed, a strict interpretation of the GDPR means that artificial intelligence is illegal.

The US model has avoided this kind of collateral damage because it has focused regulatory resources on actual risks and harms to consumers rather than assuming that all data collection is suspect and must be regulated with a one-size-fits-all approach. Moreover, America's federal policy process requires significant buy in from the major stakeholders before proposals can become law. This ensures greater compliance to the law and hence greater trust in the system.

The GDPR's compliance costs are high, about $3 million for medium to large enterprise. An estimated 20 percent of firms will probably never comply because of this high cost. Winn noted that European data protection authorities are woefully underfunded given their mandate to regulate information in the public and private sectors. Indeed, the OPCL budget to ensure compliance for 100,000 DOJ staff is larger than that of a typical European data protection authority.

This is important to keep in mind as reports suggest that a low-end estimate of the implementation costs of the California Consumer Privacy Act is $100,000 per firm. A preliminary cost-benefit analysis suggests that at this level, the cost is four times greater than the projected benefit.

Any comprehensive federal privacy legislation should be informed by all stakeholders and be based on reasonable standards for consumer preferences and legitimate uses of information. It should avoid adversarial notions of privacy as control and instead create structures that promote trust. It also requires a real-world discussion about the costs of implementation, for without compliance to the law, there is no trust.

Winn thinks deeply about these issues and has authored a number of related articles, which can be found here, here, and here.

Highlights from AEI's event on data privacy

Roslyn Layton | April 10, 2019 | AEIdeas
http://www.aei.org/publication/highlights-from-aeis-event-on-data-privacy/

Last week, AEI hosted a thought-provoking event on data privacy and protection. The full event can viewed here, and the following are some highlights.

Commissioner Christine Wilson, Federal Trade Commission

Commissioner Wilson is a veteran in antitrust and consumer protection, having served earlier at the agency under FTC Chairman Timothy Muris. She described how the FTC is an "R&D institute" for the practice of regulation and competition policy. She highlighted important points to keep in mind for federal privacy legislation, not the least of which is the need for regulatory predictability and certainty in the marketplace. It would be untenable for a firm to comply with

the 94 different online privacy laws currently making their way through state legislatures, so it is critical for Congress to act to ensure a common standard, and ideally to include common carriers and non-profit organizations in the FTC's jurisdiction.

Wilson noted that the problem of information asymmetry (a situation in which one party in a transaction has information that the other doesn't have) has not been alleviated with transparency alone, as consumers do not read lengthy privacy disclosures. She suggested that the FTC's extensive consumer privacy education resources (in both English and Spanish) could play a role to help consumers be more informed about their privacy choices. Similarly, the FTC can use educational tools to help business do a better job to protect consumers, coupled with civil penalty authority to punish bad actors. Indeed, pure command and control approaches such as the EU's General Data Protection Regulation have demonstrated downsides, such as reducing competition and venture capital. Wilson noted that the FTC's strength is its ability to support businesses "to think," underscoring America's innovative information economy. As policy improves and definitions of personal information can be clarified, ideally Congress can create a single bill that addresses both privacy and security, issues which are inherently intertwined.

Pam Dixon, World Privacy Forum

Pam Dixon, the founder and executive director of World Privacy Forum is a leader in the field of medical data breach notification and author of the groundbreaking reports The Scoring of America, One-Way-Mirror Society, and A Failure to "Do No Harm," and the book Surveillance in America. She described how command and control style frameworks are appropriate for some situations (e.g., a victim of domestic violence must assume a new identity and her old social security number must be expunged), but not others. Applying the data protection rules for a 500-bed hospital to an individual family doctor practice is not appropriate. She described how Ostrom multi-stakeholder governance models can evolve a common framework for both entities. Dixon has worked with this model and the Organization for Cooperation and Economic Development to develop guidelines on artificial intelligence. Dixon warned against the EU's

GDPR approach, which could possibly ban AI, noting the importance of developing a workable framework to prevent China from superseding the US on this front.

Peter Swire, Georgia Institute of Technology

Swire, a leading scholar and author of Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information, in Privacy and Self-Regulation in the Information Age described how, at the end the 1990s, US actors took the lead on online privacy frameworks for large enterprises but failed to follow through, leaving a vacuum of global leadership. As other nations adopt rules, they take Europe's framework, not America's.

Swire talked though a model of preemption (detailed here) that could preserve innovation incentives and sectoral knowledge without burdening enterprises with undue compliance costs. Sectoral privacy codes would be developed and approved by the FTC, and industry could evolve with them. Notably, the Children's Online Privacy Protection Act uses this approach, as did the US-EU Safe Harbor Framework, which seamlessly facilitated $250 billion in digital trade across the Atlantic, until 2015.

Swire noted that any state or federal privacy legislation may face litigation, whether in relation to free speech (see Sorrell v. IMS Health Inc.), the Dormant Commerce Clause (which he believed less likely given that states have police power), or private right of action. Notably, plaintiffs would not have standing to sue unless they could show economic harm (see *Spokeo*, Inc. v. Robins).

Bret Swanson, AEI

Bret Swanson observed that the trouble with today's economy is not that there is too much use of data, but too little. A lack of information intensity is holding back the so-called "other 70 percent" of American economy, sectors such as transportation and health care, the latter of which

consumes almost one-fifth of gross domestic product. Outside of certain applications, the traditional healthcare industry is woefully inefficient; digital industries are eight times more productive and innovative.

A summary of the Department of Justice's Peter Winn's remarks from this event can be found here.