Questions for the Record before the House Committee on Energy and Commerce
Subcommittee on Consumer Protection and Commerce
On Protecting Consumer Privacy in the Era of Big Data

How the US Can Leapfrog the EU

The Role of Technology and Education in Online Privacy

Roslyn Layton
Visiting Scholar

March 27, 2019

Chair Schakowsky, Ranking Member McMorris Rodgers, and Members of the Committee, thank you for the opportunity to provide additional testimony for the record. Please find my answers to your questions. For ease of reading, the answers to the questions are organized by the respective Committee member.

Contents

Congresswoman Robin L. Kelly

1. Many proposals direct the FTC to establish rules to address advertising practices that result in discrimination. Do you have ideas in mind for what kind of rules the FTC could put in place?

Answer:

The Federal Trade Commission (FTC) has made a detailed report on this issue.[1] There are a formidable set of laws already which protect against harmful discrimination in advertising. The report notes how the Fair Credit Reporting Act and Equal Opportunity Laws protect against discrimination in advertising. Indeed, there is a risk that regulation which reduces the amount of information for decision making could create worse outcomes by increasing prices across the board to compensate for inaccuracies. This adverse outcome was found in a study of home loans in the San Francisco Bay Area in which counties which had the strictest privacy settings ended up paying more for mortgages and defaulting at a higher rate because the banks could not accurately match the applicant to the appropriate loan.[2]

Rather than restrict firms int their ability to use data, the FTC and other policymakers should

[1] https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf

[2] Jin-Hyuk Kim & Liad Wagman, Screening Incentives and Privacy Protection in Financial Markets: A Theoretical and Empirical Analysis, 46RAND J.OF ECON.1 (2015). This is consistent with the more general phenomenon of risk-based lending markets. See Wendy Edelberg, Risk-Based Pricing of Interest Rates for Consumer Loans, 53 J.MONETARY ECON.2283 (2006)

encourage firms to improve the accuracy of their tools. Additionally, the effort should be bolstered with improving the readability of disclosures on business practices and consumer education about how online platforms work (discussed in another QFR), so that consumers can make better decisions about the online platforms they use.

Importantly the FTC report notes the importance of harnessing data practices for the betterment of the disadvantaged.

> *Businesses have strong incentives to seek accurate information about consumers, whatever the tool. Indeed, businesses use big data specifically to increase accuracy. Our competition expertise tells us that if one company draws incorrect conclusions and misses opportunities, competitors with better analysis will strive to fill the gap. . . Therefore, to the extent that companies today misunderstand members of low-income, disadvantaged, or vulnerable populations, big data analytics combined with a competitive market may well resolve these misunderstandings rather than perpetuate them. In particular, a company's failure to communicate premium offers to eligible consumers presents a prime business opportunity for a competitor with a better algorithm. To understand the benefits and risks of tools like big data analytics, we must also consider the powerful forces of economics and free-market competition. If we give undue credence to hypothetical harms, we risk distracting ourselves from genuine harms and discouraging the development of the very tools that promise new benefits to low income, disadvantaged, and vulnerable individuals.*[3]

Improving the FTC's enforcement capabilities overall, notably with removing common carrier and non-profit exemptions, increasing the FTC's budget and headcount for online privacy investigations and enforcement, and allowing the FTC to levy civil penalties, would be helpful on this issue.

[3] Supra FTC

Congresswoman Anna G. Eshoo

1. On June 28, 2018, then-Governor Jerry Brown signed into law A.B. 375, the California Consumer Privacy Act of 2018 (CCPA). A.B. 375 was first introduced by Assembly Member Ed Chau in 2017. A significant portion of the final law was adapted from a ballot initiative that was based on two years of research and was fist submitted to the Attorney General of California in 2017.

During the hearing you stated that the CCPA is "a law that came together in one week." For the record, please substantiate this statement.

Answer:

A.B. 375 was a highly flawed bill which attempted to reinstate the Federal Communication Commission's ISP-only privacy rules, following their rejection under the Congressional Review Act.[4] The FCC never conducted an assessment of the broadband providers' privacy which would suggest that Federal Trade Commission's rules were not working nor did it have a record of complaints that ISPs had violated consumers' privacy. Indeed, the only reason that the FCC invented these rules was that the classification of broadband under Title II triggered the common carrier exemption, negating the FTC's jurisdiction. The FCC's move was reckless, as it left consumers with no privacy protections, and it enshrined a regulatory asymmetry in creating two different standards for online privacy, something which is confusing and opaque for consumers. Moreover, it created a de facto market entry barrier to the oligopoly advertising market dominated by a handful of California based platforms.[5] Fortunately, the bill was withdrawn, but it likely violated the Constitution.[6]

The claim regarding the one-week deliberation is noted by Santa Clara University Law Professor. It was reiterated by more than 40 California based privacy professionals and lawyers. See Goldman, Eric, An Introduction to the California Consumer Privacy Act (CCPA) (July 9, 2018).

[4] https://www.forbes.com/sites/roslynlayton/2018/08/20/californias-internet-policy-may-have-good-intentions-but-is-it-progressive/#563247d2f450

[5] http://www.aei.org/publication/fcc-privacy-regulation-will-limit-competition-market-really-needs-online-advertising/

[6] http://www.aei.org/publication/californias-privacy-proposal-failed-but-it-probably-violated-the-constitution-anyway/

Santa Clara Univ. Legal Studies Research Paper. Available at SSRN: https://ssrn.com/abstract=3211013 or http://dx.doi.org/10.2139/ssrn.3211013

The view that the CCPA was hastily pasted together is also the Senate testimony of Evan Engstrom, Executive Director, Engine Advocacy and Research Foundation in San Francisco. He noted to the Senate Commerce Committee,

> *While CCPA's objectives are laudable, the process leading to its passage was not. Although the ballot initiative's authors clearly spent considerable time on their proposal, the legislature spent less than a week translating the initiative's general ideas into actual bill text. As a result, California legislators were unable to fully evaluate the bill, its impact on California's startup community, or its actual value to consumers. This rushed process resulted in a well-intentioned law that is full of typos, contradictions, security loopholes, and vague obligations.*[7]

Engine detailed further concerns about the CCPA threatens startups with the California Attorney General and the Senate including but not limited to

1. The overly broad definition of personal information that does not explicitly exclude de-identified and aggregated data
2. The CCPA defines "sale" expansively, covering many commonplace practices that businesses5rely on to provide goods and services to consumers.
3. The prohibition on differing service based on consumer privacy choices. In practice, this language would greatly limit the ability of companies to monetize free services, which would have a disproportionate impact on startups.
4. Privacy and security problems with CCPA's right to access and delete which create opportunities for fraud or needless requirements for additional data collection.
5. The private right of action creates uncertainty for startups. No matter how thorough a company's data security practice safe, determining whether they were legally "reasonable" is not amenable to early adjudication in a lawsuit.
6. CCPA's small business exemption fails to capture startups.
7. The design and procedure of the opt-out function does not sync with startups practices
8. The CCPA imposes significant compliance burdens for the diverse business models represented in California's startup ecosystem.[8]

[7] https://www.commerce.senate.gov/public/_cache/files/949f1fc8-dc28-4760-9f47-6cb925a1549e/0AE3566F5899E50A6C4D08C7142D8752.testimony-of-evan-engstrom-engine.pdf

[8]

Give that internet startups are the lifeblood of Silicon Valley, these concerns about the CCPA should be addressed.

2. As we learned in the recent investigations of Motherboard and the New York Times, wireless carriers and apps are selling users' location data to hedge funds, bail bondsmen, bounty hunters, and stalkers. It's likely that your personal location data and mine are also being sold without our knowledge or consent. While some companies admit they sell user data, that information is usually buried deep in 10,000-word privacy policies that are hard to find and even harder to understand.

How, exactly, would transparency and consumer education, which you stress in your testimony as central to privacy legislation, solve the problem of data being used in egregious ways, even when companies disclose such practices?

Answer:

Following is a discussion of how to create policy with realistic conceptions of consumers, their different needs and capabilities, as well as how education and transparency can complement online privacy legislation. I do not suggest that education and transparency by themselves are sufficient or are substitutes for comprehensive federal privacy legislation (while they could be for some consumers), but I wish to underscore the point that consumers are not monolithic. They can learn, evolve, and change behavior. This is important to recognize in conceptualizing any regulation on the disclosure of data practices.

The current policy process on consumer privacy has been open and inclusive, surfacing the views of many stakeholders. While there is a understanding of different kinds of firms and organizations which collect data (large Silicon Valley platforms, Fortune 1000 firms, data brokers, small and medium-sized internet companies, public sector agencies, startups, non-profit organizations, individual blogs, websites etc.), the people who use these digital products and services are lumped into single box such as "consumers" or "users". Nevertheless, consumers have multiple parameters by which they can be described including age, gender, race, occupation, education, location, affiliation and so on.

Conceptualizing consumers as a monolithic group as if they all want the same regulation is wrong. This presumption can lead to misguided policy which ultimately fails to achieve its

https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/5c87c83c6e9a7f38beb04d5c/1552402492673/Engine+-+CCPA+comments.pdf

stated goals, or to which firms and consumers find workarounds. Users of online services are highly diverse, have different preferences, and make individual, contextualized decisions based upon how they perceive the transaction with their data. Research tools deployed among hundreds of millions of users shows that privacy preferences change minute to minute depending on the site visited, the user's goal, and the user's desire for security and speed.[9] Users interpret privacy within a context, and many don't object to sharing information per se, only to sharing that is inappropriate based on the context.[10]

While there is a benefit to a single, comprehensive standard, policymakers should realize that not all "consumers" are the same. The point is underscored by a leading data broker's categorization of consumers by "lifestage", affluence, and use of digital technologies.[11] American households are further categorized into 70 segments and 21 groups based on similar demographic, socio-economic and consumer behavior.[12] Hispanic consumers can be categorized into 55 specific buying groups.[13] Understandably some regulatory advocates are opposed to such tools, even though they have been integrated in the American economy for decades, and prior to that, were conducted via analog means.

The point is merely that a data broker's description of "consumers" is a more accurate reflection than the current policy discourse. As such, it is worthwhile for policymakers to try to understand the diversity of consumers before making policy. Consumer education plays an important role to fill the gap between what regulatory advocates want and what different consumers prefer. As such, it makes sense to propose a baseline set of principles and to allow consumers to supplement their preferences with informed choices.

Responsibilities of consumers. The leading textbook of the field "Economic Education for Consumers" details the notions of consumer expectations as well as consumer responsibilities.[14] They include the following concepts:

1. Responsibility to be an educated consumer, including responsibility to gather and evaluate information before making a decision

[9] Scott Meyer, "The Next $50 Billion Will Come From . . . Putting Users First," Ghostery Inc. , https://www.slideshare.net/ghosterybrand/the-next-50-billion-will-come-fromputting-users-first.
[10] HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2009), https://www.sup.org/books/title/?id=8862.
[11] "Acxiom Personicx," accessed November 9, 2018, http://www.personicx.co.uk/personicx.html.
[12] "Consumer and Household Segmentation | Personicx," Acxiom, accessed November 9, 2018, https://www.acxiom.com/what-we-do/consumer-segmentation-personicx/.
[13] Ibid
[14] Roger LeRoy Miller and Alan D. Stafford, *Economic Education for Consumers* (Cengage Learning, 2009). p. 88

2. Responsibility to use products and services safely
3. Responsibility to use information to make choices
4. Responsibility to choose carefully
5. Responsibility to express opinion about a product, as well as report improper business practices. This can be communicated to the community, firm, and/or authorities.

In addition, consumers have the freedom to consume in a responsible manner by selecting products and services that conform to their values as well as seek redress from injury by unfair, deceptive, and defective products and services.

Role of Consumer Education in Online Privacy. Consumer education is by no means a panacea. Indeed an academic review of the range of methods and approaches employed for financial literacy education notes shortcomings in their effectiveness.[15] On the other hand, the value of education to improve outcomes in personal health is well-documented.[16] However financial literacy may be more effective in imparting "rules of thumb", for example, knowing the value of diversification in an investment portfolio is more important than knowing the litany of financial instruments.[17]

It is instructive to consider the robust, vibrant market for information and education in the consumer electronics field detailing the most minute and technical aspect of machines. For decades consumers have availed themselves to magazines, online discussions, rankings, reviews, how-to videos, conferences, and so on. There is no policymaker directing the discussion, but it grows by consumer demand.

There is no reason why there could not be a similar field for the consumption of online services, which describes the contours of online privacy and how users could select different technologies to manage their privacy. The difference is that consumer electronics education is essentially funded by advertising placed by the providers of phones, devices, appliances, and so forth. In general, online platforms do not advertise as such, so there is a policy opportunity to see how such resources can be developed in the marketplace. Consumer education on privacy could help consumers understand the principles of consent and control and exercise their associated freedoms.

---

[15] Willis, Lauren E. "Evidence and ideology in assessing the effectiveness of financial literacy education." *San Diego L. Rev.* 46 (2009): 415

[16] Connell, David B., Ralph R. Turner, and Elaine F. Mason. "Summary of findings of the school health education evaluation: Health promotion effectiveness, implementation, and costs." *Journal of school health* 55.8 (1985): 316-321.

[17] Supra Willis

Public Choice Explanation for the Lack of Consumer Education on Privacy. The academic discipline of public choice uses economics to investigate problems in political science. It could help explain why consumer education on privacy is lacking, aside from one possible explanation that consumers are not interested to learn about privacy and therefore do not demand such information. A public choice theorization would likely recognize that while the notion of consumer education has implicit valence, industry and regulators may have incentives to de-emphasize education. Indeed, if consumers are empowered to make informed choices, they have less need of regulatory supervision. Similarly, consumers making informed choices also affects industry; it has a powerful effect to drive consumers from one firm to another.

The GDPR is suspect in that among its 173 provisions the role and importance of consumer education is never discussed.[18] This is a serious oversight particularly when the EU's official cybersecurity research institute noted the primacy of consumer education to create privacy, accountability, and trust.[19] Nor is consumer education discussed in the context of the California Consumer Privacy Act. This is likely because the real objective for these regulations is not empower consumers but to strengthen the data protection and compliance business, specifically to give jobs to data protection officers, regulators, and litigators.

The assumption of the European and Californian rules is that regulatory authorities have more information than consumers and firms and therefore know better how to order transactions in the marketplace.[20] All the same, the these regulations impose massive new responsibilities on data protection agencies without a concurrent increase in training or funding.[21] Data regulators must wear many hats, including "ombudsman, auditor, consultant, educator, policy adviser, negotiator, and enforcer."[22] Furthermore, these regulations widen the gap between the high expectations for data protection and the low level of skills possessed by data supervisors charged with its implementation.[23] There are certainly many talented individuals among these

[18] Layton, Roslyn, How the GDPR Compares to Best Practices for Privacy, Accountability and Trust (March 31, 2017). Available at SSRN: https://ssrn.com/abstract=2944358 or http://dx.doi.org/10.2139/ssrn.2944358

[19] Claude Castelluccia and more, "Privacy, Accountability and Trust – Challenges and Opportunities — ENISA," Report/Study, Enisa, February 18, 2011, https://www.enisa.europa.eu/publications/pat-study/.

[20] See generally F. A. Hayek, "Economics and Knowledge," 1937; and F.A. Hayek, "The Use of Knowledge in Society," 1945.

[21] Douglas Busvine, Julia Firoretti, and Mathieu Rosemain, "European Regulators: We're Not Ready for New Privacy Law," Reuters, May 8, 2018, https://www.reuters.com/article/us-europe-privacy-analysis/european-regulators-were-not-ready-for-new-privacy-law-idUSKBN1I915X.

[22] Colin J. Bennett and Charles Raab, "The Governance of Privacy: Policy Instruments in Global Perspective," 2006.

[23] Charles D. Raab and Ivan Szekely, "Data Protection Authorities and Information Technology," *Computer Law and Security Review* (forthcoming), https://ssrn.com/abstract=2994898.

ranks, but the mastery of information communication technologies varies considerably among these professionals.

Public choice theory also suggests that the data regulators' preferences are not necessarily aligned with the "public interest," or what is best for consumer welfare in the long run. Increasing user knowledge and the quality of data protection technology could legitimately make people better off, but it could also render regulators less important. While data regulators will not necessarily reject policies that improve user knowledge and technology design, it is in their interest to promote inputs that increase their own resources and legitimacy in conducting compliance and adjudication.[24]

Surveys demonstrate that many users fail to practice basic privacy-enhancing behaviors.[25] This situation is ripe for improvement and represents a classic example of how consumer education can improve outcomes better, more quickly, and at a lower cost than regulation. Indeed, the first principle of consumer education in data protection, buyer beware, is the same first principle for how citizens should protect themselves in cyberthreats in Michael Chertoff's new book on cybersecurity: "Be mindful of what data you transmit and what you connect to your own network."[26] He also recommends practicing cyber hygiene, taking advantage of layered cybersecurity technology, and outsmarting scams with a phone call.

Consumers need to practice the same kind of vigilance and personal responsibility in cybersecurity as they do in the data protection domain. Outsourcing the job to bureaucrats will not cut it, as the user can be a vulnerability point. Consider warnings and labels on food and chemicals; while regulation can mandate that disclosures be made, if users do not recognize the meaning of expiration dates or consumption warnings, then disclosure has little impact.

Transparency. The principle that "organizations should be **transparent** about how they collect, use, share, and store users' personal information" is laudable. Indeed, the FTC has been extremely deft to use transparency rules to bring actions against actors which threaten and/or harm consumers. The agency has levied significant fines and collects compensation for users. The history of enforcement serves as an important deterrent as well as a roadmap for firms.[27]

---

[24] Roslyn Layton, "How the GDPR Compares to Best Practices for Privacy, Accountability, and Trust," March 31, 2018, 14, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2944358.
[25] Layton, "How the GDPR Compares to Best Practices for Privacy, Accountability, and Trust."
[26] Michael Chertoff, "Exploding Data: Reclaiming Our Cyber Security in the Digital Age," *Atlantic Monthly Press*, 2018.
[27] "Privacy and Security Enforcement," Federal Trade Commission, July 22, 2013, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement.

The bottom line for policymakers is that the FTC has proven its capability to police privacy and security, and transparency requirements are powerful tools to protect privacy.

However imposing transparency requirements is not without costs to consumers. The GDPR is driving disclosure overkill. Indeed, European requirements have become so onerous that many consumers have stopped using websites with cookie disclosures.[28] Opera, the popular browser, has developed technology to block the disclosure dialogues that plague users every time they visit a website in EU. Indeed, technologies and users can find innovative ways to go around regulations they don't like.[29]

Policymakers should not believe that automatically making consent more explicit makes consumers more informed. If the user fundamentally does not understand to what she agrees or the underlying transaction, no amount of disclosure, however detailed or granular, empowers the user. This is the gap that consumer education can fill.

When producers and consumers do not have perfect information, this discrepancy can give rise to inefficiency or abuse. Peer-to-peer platforms have resolved many of these problems of informational asymmetry through information sharing. Consider how the ability to evaluate drivers and riders is an essential part of ridesharing apps. Before Uber, neither the taxi company nor the regulator was interested to publish real-time information about the quality of drivers or cars, as it could impugn the deficiency of regulator. Ratings and peer reviews are essential in the digital economy. Indeed, some health regulators use Yelp ratings to help inform how they deploy their inspection resources.[30]

Consumer education could be vital to demystify the "black box" of many internet platforms, which for many consumers is a system in which they can observe the inputs and outputs but have little to no insight to its internal workings. It is only when consumers have enough education about the tools they can use that they can begin to "exercise **control** over the personal information they provide to organizations."

---

[28] Daniel Castro and Alan McQuinn, The Economic Cost of the European Union's Cookie Notification Policy, ITIF, Nov. 6, 2014, https://itif.org/publications/2014/11/06/economic-cost-european-unions-cookie-notification-policy.
[29] Adam Thierer and Chand Reese. "Evasive Entrepreneurs and Permissionless Innovation. The Bridge. Sep 11, 2018 https://www.mercatus.org/bridge/commentary/evasive-entrepreneurs-and-permissionless-innovation
[30] Roslyn Layton, "How Sharing Economy Regulatory Models Could Resolve the Need for Title II Net Neutrality," AEI, June 26, 2017, http://www.aei.org/publication/sharing-economy-regulatory-models-resolve-need-title-ii-net-neutrality/; And Arun Sundararajan, *The Sharing Economy: The End of Employment and the Rise of Crowd-Based Capitalism* (*MIT Press*, 2016)

Preliminary ideas about promoting consumer education in privacy. My submission to the FTC describes some of the leading privacy education programs beginning on page 15.[31] Firms could support these organizations financially to spread the information and as an example of their commitment to principles. Following are additional ideas to consider to embedding consumer education for privacy into the marketplace.

- Leverage the FTC's educational website, materials and knowledge into the public domain https://www.consumer.ftc.gov/topics/privacy-identity-online-security. Firms could link to the FTC from their websites.
- Firms can develop their own educational platforms for privacy and engage and encourage customers to learn.
- Firms could offer rewards/discounts for customers to take online privacy training.
- Firms could supplement disclosures with consumer-centric tools (videos, cartoons etc.) to explain how their products and services, incorporate data.
- A task force of FTC, industry and consumers could promote consumer education for privacy.

Transparency and consumer education are important so that consumers can make informed decisions about whether they want to use one service versus another. Indeed, consumers may well say that they don't want to use a certain service because they are not comfortable with the provider's practices. The suggestion of supporting consumer education for online privacy follows the experience with initiatives in health education and financial literacy. If we want people to value privacy, they should be able to access tools and resources which explain why it is important and how, in basic terms, online business models work.

If companies violate their contracts and terms of service, using data that is not disclosed and/or without consent, these violations can and should be processed by the Federal Trade Commission. Improving the FTC's enforcement capabilities overall, notably with removing common carrier and non-profit exemptions, increasing the FTC's budget and headcount for online privacy investigations and enforcement, and allowing the FTC to levy civil penalties, would be helpful on this issue.

The Honorable Michael C. Burgess, M.D.

[31] https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0051-d-0021-152000.pdf

1. One of my concerns with the online ecosystem is transparency -- how companies tell their consumers about their collection and use of personal data. Terms of services are too long and too complicated for anyone to reasonably read.

    a. Dr. Layton, in your testimony you state that there is no consumer protection without consumer education. What should we be thinking about in Congress to improve consumer education initiatives?

Answer:

Please see answer to question posed by Representative Eshoo on p. 6.

2. Dr. Layton, I recently heard from a small business in Dallas/Ft. Worth, called Ultimate Ventures, that specializes in business meetings, events and logistics. This small business does not normally deal with a lot of consumer data, and is now being asked to sign a "data protection agreement" from a client based on the GDPR that – in the words of the President of the business – is "not simply daunting, but is impossible to agree to" and that there is "no way" for the company to agree to everything in the agreement.

    a. What would it mean for small businesses in the U.S. if we follow suit and adopt a framework similar to GDPR?

Answer:

My Senate testimony[32] detailed the 10 harms of the GDPR (and CCPA) already documented which include

1. Rules promised to level the playing field have strengthened the largest players.
2. Small and medium sized firms have weakened as a result of the GDPR, the opposite of the promised effect.
3. The GDPR has silenced free speech and expression.
4. The GDPR has proven cost prohibitive for many firms.
5. The GDPR threatens innovation and research.
6. The GDPR has created cybersecurity threats.

[32] https://www.judiciary.senate.gov/imo/media/doc/Layton%20Testimony1.pdf

7. The GDPR and the CCPA create risks for identity theft and may incentivize fraud.
8. The GDPR, however well-intentioned, has tricked people into thinking that they and their data are now more private and safe, when they are not.
9. The GDPR and the CCPA use the pretense of customer sovereignty to increase the power of government.
10. The GDPR and the CCPA fail to incorporate the role of innovation and education, factors which ultimately create better privacy systems and empower users to make informed decisions.

All these outcomes have either a direct or indirect impact on small business. In summary, we have seen that as a result of the GDPR, the large advertising platforms have gained market share; smaller advertising competitors have lost market share; small firms have stopped serving markets because of the cost and uncertainty of regulation; and small firms have been disincentivized to pursue technical means which could ultimately improve privacy because of the lack of a safe harbor to test new technologies.

b. What concerns do you have with the California privacy law and its effects on small businesses?

Answer:

The costs of the CCPA is likely to be at least four times its benefits. Firms are spending a minimum of $100,000 today to comply with the CCPA. It is expected that there are half a million firms liable under the CCPA; they are overwhelmingly small to medium sized businesses; most spend but a few thousand dollars annually on their information technology operations and likely have zero budget for privacy regulation. Even with the minimum revenue threshold, the CCPA will cause many firms to do one of the following: 1. Stop serving California; 2. Look for a buyer or another form of exit; 3. Close down. The CCPA is particularly unfair because it was conceived to discipline giant Silicon Valley firms with market caps that exceed the gross domestic product of most countries, but its many requirements fall the hardest on small and medium sized firms which, not only do not have budget to pay for costly software upgrades and privacy

lawyers, but have not compromised the privacy of their users. It is not the first time that regulation promised to protect consumers ends up rewarding large, incumbent industries.[33] This dynamic has been experienced with the airline, telephone, and train industries, and California policymakers now make the same mistake with internet platforms.

The preliminary analysis for the benefit cost of the CCPA is available at http://www.aei.org/publication/the-costs-of-californias-online-privacy-rules-far-exceed-the-benefits/ and follows below.

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.

[33] Should tech giants be more heavily regulated? Debate in Economist.com 30 April – 7 May 2018. Follow up mention on "Open Future" https://www.economist.com/blogs/openfuture/2018/05/open-future

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.

Small Business Testimony to the Senate

Sen. Jerry Moran, (R-KS), Chairman of the Subcommittee on Manufacturing, Trade, and Consumer Protection, convened a hearing on Small Business Perspectives on a Federal Data Privacy Framework. The testimonies of this hearing are worthy of review. Here are a few of the highlights. Here are some of the perspectives shared at the hearing.[34]

National Association of Realtors

Nina Dosanjh, Vice Chair of the Technology Policy Committee of the San Francisco based National Association of Realtors (San Francisco) observed, "Realtors, like many main street businesses, rely on data to enhance revenue and drive efficiency, whether by better understanding the needs of existing customers, reaching new ones, or obtaining valuable insights to guide a wide array of business decisions. For example, realtors may use consumer data to allow them to advise their selling clients on how to price their home and how many potential buyers will be interested at different price points. It can also be used to give buyers a better sense of what types of properties competing home buyers are looking at, as well as their buying ability. In sum, realtors use the consumer data they collect to improve their clients experience in a way that consumers can understand and expect."

Silver Star Communications

[34] https://www.forbes.com/sites/roslynlayton/2019/03/26/congress-investigates-whether-privacy-rules-can-protect-consumers-without-killing-small-business/#7217e9c34459

Jefferson England the CFO of Silver Star Communications, headquartered in Thayne, WY, explained the need for a single federal standard that allows for companies to serve their customers. “We provide services in multiple states, and having to manage a patchwork of state privacy laws will not only create an environment of uneven protections, but would create administrative burdens on small business,” he said. "Legislation should not interfere with business and consumer relationships that are based on mutually understood privacy protection tolerances. If a consumer is willing to release data in order to receive services, it should be the consumer’s right to do so, and the business should be allowed to provide such services. Similarly, the market should be allowed to present data privacy alternatives as competitive differentiation so long as data privacy protection practices are clearly identified and accepted by the consumer."

Engine Advocacy and Research Foundation

Evan Engstrom, Executive Director, Engine Advocacy and Research Foundation, the so-called voice of Silicon Valley startups, suggests maintaining the spirit and good intentions of the CCPA without its heavy-handed prescriptions. His testimony offers highly detailed assessment of the regulatory impact to startups and details the impact to date of the GDPR. He observes, "... as state and federal policymakers look to bolster privacy protections for consumers, there is a very real risk that the end result will be a complex regulatory landscape that startups on bootstrap budgets can’t afford to comply with, especially compared to large companies with massive budgets and legal teams. Rules that are ostensibly pro-privacy could end up cementing the market power of those very Internet giants whose behavior sparked much of these conversations. . .We’ve seen this with the European Union’s General Data Protection Regulation, where many small companies left European markets or abandoned plans to expand to European markets rather than face the costly compliance burdens. In fact, there’s concrete evidence that GDPR gave the big Internet companies a boost in Europe. According to one survey, Google’s ad tracker actually saw an increase, albeit small, in reach since GDPR went into effect ten months ago. Facebook’s ad tracker saw a small decrease, but everyone else saw significant losses. GDPR’s extensive and complex obligations created new compliance burdens that large incumbents could bear but resource-constrained startups could not. Policymakers should enshrine consumer privacy protections in law, but they must work to ensure far-reaching rules promote consumer welfare without harming competition."

Engstrom details the many ways that the CCPA threatens startups including but not limited to

1. The overly broad definition of personal information that does not explicitly exclude de-identified and aggregated data

2. The CCPA defines “sale” expansively, covering many commonplace practices that businesses5rely on to provide goods and services to consumers.
3. The prohibition on differing service based on consumer privacy choices. In practice, this language would greatly limit the ability of companies to monetize free services, which would have a disproportionate impact on startups.
4. Privacy and security problems with CCPA’s right to access and delete which create opportunities for fraud or needless requirements for additional data collection.
5. The private right of action creates uncertainty for startups. No matter how thorough a company’s data security practice safe, determining whether they were legally “reasonable” is not amenable to early adjudication in a lawsuit.
6. CCPA’s small business exemption fails to capture startups.
7. The design and procedure of the opt-out function does not sync with startups practices
8. The CCPA imposes significant compliance burdens for the diverse business models represented in California’s startup ecosystem.

Kansas City Tech Council

Ryan Weber, President of the Kansas City Tech Council dispelled the view that big data is only something for Silicon Valley firms, "Algorithms are the backbone of most modern technology applications, and algorithmic thinking is necessary when considering the future of federal data privacy laws. Conditional algorithms use IF-THEN decisions between two courses of actions. For example, IF a company, no matter the size collects sensitive data, THEN it must comply with federal data privacy laws and meet certain cybersecurity standards set forth by the appropriate regulatory agency. As technology continues to advance and find its way into every industry, business sector, and company, we must remember, not all technology is created equal and not all data should be treated the same. Accountability will make federal data privacy laws effective. The agency responsible for upholding these laws should be allowed to adjust fines and penalties equal to the violation. This sentiment is shared by our member companies. Other global examples of privacy laws, such as General Data Protection Rights (GDPR), set fines at such a high-level many small and startup companies cannot afford."

The Honorable Richard Hudson

1. Dr. Layton, the California law does not allow a company to deny, or charge a different price, or offer a different quality of goods or services to consumers who do not want a company to collect data. This raises some government takings questions but how will this impact lower income families? Will companies be forced to provide free services to California consumers, paid for by the rest of America?

Answer:

Thank you for asking this important question, which does in fact implicate government takings. It also reflects many privacy advocates' absolutist view of privacy rights which threaten to eclipse other rights, notably an individual's right to decide for himself or herself what kind of business model she wants to access.[35] The prohibition on commercial freedom in the CCPA is a feature designed by CCPA advocate Alastair MacTaggart who described in his questioning in his Senate hearing that he took offense that his local Supercuts salon requesting his email and phone upon checking in for an appointment.[36] MacTaggart called it "out of control" and intimated that this practice should be eliminated for all Supercuts customers. (He also spent nearly $3.5 million of his own fortune from a successful real estate business, which, ironically, relies on the same kind of data processing he now wants to eliminate.) This kind of elitism fails to see how many people appreciate SMS reminders for their salon appointments and want to receive email offers of coupons for hair care products, discounts, and so on.

When the law requires a firm to provide a service without collection of data it creates a free rider problem in which those who consent to data collection must endure increased data collection and processing to compensate for those who don't consent. As such, it unfairly burdens consenting users to higher burdens and costs without commensurate benefit. More generally, it decreases the parameters of competition, precisely the innovative ways which small firms could differentiate with data in order to gain a foothold in the marketplace.

The question alludes to fundamental theories of privacy. Online privacy can be seen from two competing paradigms. One model is that of rational choice, in which the individual weighs the cost and benefits of privacy and decides whether to transact. The other view paints users as being at the mercy of external factors that determine whether they reveal or conceal themselves. The former tends to support solutions and technologies that empower consumers to make their own choices and suggests that firms, valuing their customers, will take proactive steps to steward their experience. The latter holds that privacy tools are inevitably unreliable and that firms take predatory advantage of users. According to this view, regulation is needed to keep firms in check and to protect consumers.

[35] https://www.libertarianism.org/building-tomorrow/protecting-data-privacy-without-destroying-the-internet

[36] https://www.commerce.senate.gov/public/index.cfm/hearings?ID=3A98134B-6CCE-4491-B22B-BC831C3DFF5D

Empirical tests of the two models show that consumers are not inevitably predisposed to making bad choice or failing to act in a privacy enhancing matter.[37] Research from tools deployed among hundreds of millions of users shows that privacy preferences change minute to minute depending on the site visited, the user's goal, and the user's desire for security and speed.[38] As such, the opt-in regime is not empirically demonstrated as superior means of protecting the user's privacy. The point is merely that privacy is not a binary choice. There are many means and modes to secure, and its importance varies depending on the user and the situation. As such, policymakers should tread carefully before applying draconian regulations that may satisfy the most vocal privacy advocates but reduce benefits and utility for millions of consumers.

Notably a review of the literature on the impacts of economic regulation in the information communications technology sector shows a detrimental impact of regulation on innovation.[39] Regulation can create a deadweight loss in the economy as resources are diverted to regulatory compliance and away from welfare-enhancing innovation. A study across all major industries from 1997 to 2010 found that less-regulated industries outperformed overregulated ones in output and productivity and grew 63 percent more. Overregulation increases barriers to entry for entrepreneurs, which slows economic growth.[40] Moreover, regulation can crowd out efforts to create new and better systems.[41] For example, under the GDPR firms must employ privacy professionals, reducing revenue for engineers who can design and deploy privacy professionals.

Notably Engine Advocacy and Research Foundation has answered this question in its testimony to the Senate Commerce Committee, calling it "Prohibition on differing service based on consumer privacy choices."[42] They declare,

> CCPA prohibits companies from offering different prices or levels of quality of products and services to consumers who exercise their rights under the law, including

[37] Idris Adjerid, Eyal Peer, and Alessandro Acquisti, "Beyond the Privacy Paradox: Objective Versus Relative Risk in Privacy Decision Making," April 14, 2016, https://ssrn.com/abstract=2765097.

[38] Scott Meyer, "The Next $50 Billion Will Come From . . . Putting Users First," Ghostery Inc. , https://www.slideshare.net/ghosterybrand/the-next-50-billion-will-come-fromputting-users-first.

[39] Luke Stewart, "The Impact of Regulation on Innovation in the United States: A Cross," Information Technology and Innovation Foundation, June 2010, 18, http://www.itif.org/files/2011-impact-regulation-innovation.pdf.

[40] Antony Davies, "Regulation and Productivity," Mercatus Center, May 7, 2014, https://www.mercatus.org/publication/regulation-and-productivity.

[41] Patrick McLaughlin and Richard Williams, "The Consequences of Regulatory Accumulation and a Proposed Solution | Mercatus," Mercatus Center, February 11, 2014, http://mercatus.org/publication/consequences-regulatory-accumulation-and-proposed-solution.

[42] https://www.commerce.senate.gov/public/_cache/files/949f1fc8-dc28-4760-9f47-6cb925a1549e/0AE3566F5899E50A6C4D08C7142D8752.testimony-of-evan-engstrom-engine.pdf

the right to opt-out of data sharing. In practice, this language would greatly limit the ability of companies to monetize free services, which would have a disproportionate impact on startups. Unlike large Internet companies that have been offering ad-supported free services for years, a startup entering the market will have a harder time getting new users who are unfamiliar with the company to pay for its products and services. Even if a startup can get some users to pay, the law would effectively require every ad-supported company to take on the burdens associated with establishing a payment processing system in case some users decide to opt-out. At the same time, a small company will have significantly fewer opportunities to offset the costs of offering a product or service for free using revenue streams from other parts of its business, while bigger companies are better positioned to take a loss on offering a free product or service. The law does allow companies to charge a different rate or offer a different level of products or services so long as "that difference is reasonably related to the value provided to the consumer by the consumer's data." While this phrasing is likely a drafting error and obviously unworkable—how could a company know how much an individual consumer values his own data?—even a generous reading of the law's presumed goal would present existential problems for small startups. Even if companies are forced to provide service to consumers who opt-out of data sharing practices that are fundamental to the company's business model, but are allowed to recoup the lost value directly from consumers by charging a different price or offering a different level of service so long as that difference is reasonably related to the value provided to the company by the consumer's data, startups would have a very difficult time estimating or defending in court what would constitute a price or quality difference that's "reasonably" related to the value of a consumer's data. As startups launch and grow their businesses, there's typically not an immediate, obvious value that can be clearly assigned to individual pieces of data supplied by consumers. Even if a data set has an explicit value in the eyes of investors, data associated with any particular consumer typically does not hold much value on its own.

Even worse, this non-discrimination provision would require every company that shares User data to build the infrastructure to process customer payments in the off chance that a particular consumer opts-out of the company's data practices but wishes to pay a "reasonably related" fee instead. Larger companies might be able to bear the increased overhead of payment processing, but smaller startups will not.