August 20, 2018
Submission to the FTC Hearings on Competition & Consumer Protection
Request for Comment
Responsive to Topic 4

The following compilation is comprised of summaries of articles identified by students at Santa Clara Law School in response to RFC Topic 4, *The Intersection between Privacy, Big Data, and Competition*. Each description includes a summary of the article, the student's opinion of the article, and, where available, the author's contact information.

Respectfully submitted,

Professor Colleen Chien on Behalf of Santa Clara Law School Students

==========

**Response to 4a**

data as a dimension of competition, and/or as an impediment to entry into or expansion within a relevant market

1. Big Data and Competition Policy (CERRE, 2017)
   - Summary: Big data may have anti-competitive potential depending on the accessibility and value of the data. While standard competition policies (in the EU) may be sufficient to deal with personalized online ads, data may still inadvertently create an anti-competitive barriers to entry in other ways. Data can potentially create barriers to entry by drastically improving the "first-move" advantage. If the data collected can be positively fed back into improving the application, the first successful application will quickly outpace all other competitors. We can observe some of these effects in the lack of any true competitor to Google's search service. However, as the author notes, the data Google collects is not impossible to recreate and improvements on AI and technology are not fueled solely by data. Thus, in reality a myriad of factors ultimately determine market dominance. In order to regulate such "first move advantages" one must understand the underlying technology and utilize a case-by-case approach. The article also discusses personalized (a) price discrimination and (b) targeted ads. The former has not been observed in the EU and the latter is influenced by GDPR. Compliance with GDPR creates inherent difficulty of entry, since all must comply with its more stringent provisions. However, the literature is unclear on whether targeted advertisements are actually detrimental to consumer welfare. As the effects of any action taken have yet to be studied, the authors recommend avoiding regulation or action that might stifle innovation over explicit regulation. In summary, there are a lot of factors that play into whether data is being used in an anti-competitive way. Regulatory agencies should seek to understand the underlying value of the data prior to regulation.
   - Opinion of the article: Interesting piece describing the intricacies of competition policy and big data in the EU. The author cites quite a few studies and information which makes the article a good starting point for international comparative law. The author also provides insight into how scholars are viewing big data and breaks down where big data might create anti-competitive environments and what factors to look out for (using EU as a backdrop).
     Quite a nice survey piece with an interesting take on the value of data and provides factors for its proper valuation.
   - Author/Affiliation/Contact information: Marc Bourreau, Alexandre de Streel, and Ingre Graef, *Big Data and Competition Policy*, Center on Regulation in Europe,

.

Responses to 4b

competition on privacy and data security attributes and the importance of this competition to

consumers and users (focus on the GDPR)

1. Embrace the GDPR To Gain A Competitive Edge - Leverage New And Updated Privacy Laws To Win, Serve, And Retain Customers (Forrester, 2017)

- Summary: Even though many companies may think about the new General Data Protection Regulation (GDPR) as a burden, Forrester related to over 200 previous studies and conducted a study stating that data security and privacy rules can give businesses a competitive advantage opening up business benefits that boost return on investment, such as improved customer loyalty and more efficient operations. According to Forrester, the biggest challenge companies (39%) see in the new GDPR is balancing compliance with exceptional customer experience. Nevertheless, firms believe they will ultimately benefit from compliance because customers will be "happier, more loyal and engaged". Thirty-five percent of firms expect to see improved customer satisfaction, 34% expect increased customer loyalty, and 30% expect more engaged customers because of compliance with the privacy regulations. Furthermore, along with a brand lift "thirty-two percent of firms expect the perception of their brand to improve as a result of GDPR/ePrivacy compliance", which could lead to greater brand differentiation in the marketplace. All in all, Forrester thinks GDPR will constitute a win-win-situation for both businesses and customers.
- Opinion of the article: As an exchange student from Switzerland I found it interesting to read about the GDPR from an "American perspective". In my home country, which is surrounded by EU-states the GDPR is a very contentious topic as it forces politics to partly take over EU norms to stay competitive. In my opinion, the Forrester study offers an interesting view on how businesses can make the GDPR a competitive advantage. On the other side, I doubt that this study is unbiased as it was originally published by Evidon. Further, the argumentation "firms believe that…" does not convince me: How can something be a competitive advantage if everyone who is doing business in the EU needs to apply with the GDPR?
- Citation/Author/Affiliation/Contact information: A Forrester Consulting Thought Leadership Paper Commissioned By Evidon December 2017 *retrieved from* https://www.evidon.com/wp-content/uploads/2017/12/Evidon-GDPR-Report-12_2017.pdf Project Director: Rachel Linthwaite, Market Impact Consultant

2. Fighting Cyber Crime and Protecting Privacy in the Cloud (Bigo et al 2012)

- Summary:
  - The study starts by investigating the issues at stake when dealing with cloud computing
  - Currently, the EU framework on cloud computing in relation to cybercrime lacks a clear sense of direction, priorities and practical coordination
  - This study therefore examines in depth what is at stake from the perspective of data protection and privacy
  - Main concern for private citizens, companies and public administration using cloud technologies is in the management of the data over the possible increase in cyber fraud or crime.
  - With cloud-computing infrastructures mainly owned by companies, the main challenge is the rights of individuals whose data is being processed.
  - In the field of cybercrime, the challenge of privacy in a cloud context is underestimated, if not ignored. Data protection laws appear to be very marginal and inadequately addressed to meet the challenges of privacy.
  - Cloud computing and cybercrime pose legal challenges to fundamental legal concepts in the fragmented EU legislative framework.
  - One solution is an accountability approach that will imply the responsibilities, liabilities and obligations vested upon every actor with considerable power.
- Opinion of the article: This study/article was a good read in understanding the issues/challenges with cloud computing and how these issues are being addressed (or not addressed) by agencies.

With the Internet being the communication mainstream of the world, the data privacy of all entities is a very important topic. It is concerning how nations are not taking greater measures in establishing laws/regulations to protect people's data/privacy.

- Citation/Author/Affiliation/Contact information: Bigo, D., Boulet, G., Bowden, C., Carrera, S., Jeandesboz, J., & Scherrer, A. (2012). Fighting cyber crime and protecting privacy in the cloud. Brussels: European Parliament.

3. Privacy in a Digital, Networked World (Privacy in Mobile Devices) (Zeadally 2015)
   - Summary: The article details the high-level issues facing the mobile industry going into the deeper issues with location tracking, implicit and explicit data collection, and the challenges and the opportunities the industry faces. With respect to the surveillance the paper discusses that it is constant when a party uses any application on their mobile device. Users will usually consent to the collection of the data by using the service, but most users are also subject to other forms of collection where apps will access information without consent of the user. This information access can come in the form of web tracking, or access to the user's contacts inside of the phone. The data leaks section goes into three major types of leaks, business policy, permission and embedded content leaks. Each of these leaks lets user data out for the benefit of either the application or some third party which will utilize the data for its own economic purposes, legal or illegal. The article further details how the user can fight back, such as disabling cookies, but this limits the usefulness of the servies. Finally, the article discusses the upcoming challenges, such as shifting to privacy by design to protect data.
   - Your opinion: The article does a good job of giving an overview of the issues facing the mobile platform from both an engineering and policy standpoint. My major takeaway is that there has been little incentive for the industry to adopt better privacy guidelines as the use of data has thus far been a big money maker with little downside for the leaks. Thus, there is a need for better penalty mechanisms or industry practice to ensure that user's data is not leaked/abused.
   - Privacy in a Digital, Networked World [electronic resource] : Technologies, Implications and Solutions / edited by Sherali Zeadally, Mohamad Badra. "Privacy in Mobile Devices" (2015) Springer International Publishing. Page 207. ISSN 2197-8433
     e-mail:
     e-mail:

**Responses to 4c**

whether consumers prefer free/ad-supported products to products offering similar services or capabilities but that are neither free nor ad-supported

1. Free Fall: the Online Market's Consumer Preference Disconnect (Strandburg, 2013)
   - Summary: Article explores the relative efficacy and invasiveness of different types of online advertising: including undirected or "run-of-network" (wide circulation), contextual (tied to a context), and behavioral (calibrated to the individual and their behavior); the techniques differ in how privacy invasive and effective they are. Summarizes articles that show that: behavioral advertising and effectiveness of same went down after the European privacy directive (Goldfarb-Tucker), behavioral advertising is more effective in the short term (Yan), users say they don't want customized ads (Turow) and find customization invasive (McDonald/Cranor) - but they largely also won't take action to eschew customization. It also discusses the ways in which the internet changes paid vs. advertising/free models of content distribution (@122 et seq), the ways in which Internet users don't have the ability to assess the "price" of the advertising-based transactions because, unlike a cash exchange at the point of sale, consumers are subject to "ongoing and silent data collection in connection with their ongoing use of online products and services" and the limits of "notice and choice principals" as implemented through privacy policies. In Section IV, article discusses whether or not behavioral advertising is really necessary/what the consequences of banning it might be, acknowledging that it free products create enormous value (2010 IAB estimate of $130B), and suggests that moving to such a model would require

collective/regulated action.

- Opinion of the article: an excellent overview of the issues that incorporates the empirical research that, though dated, explores the tradeoffs between different types of advertising-supported content models and their regulation.
- Citation/Author/Affiliation/Contact information: Strandburg, Katherine J., "Free Fall: the Online Market's Consumer Preference Disconnect" (2013). New York University Public Law and Legal Theory Working Papers. Paper 430. http://lsr.nellco.org/nyu_plltwp/430 Prof. Kathy Strandburg, NYU Law School,

2. The Federal Trade Commission and Consumer Privacy in the Coming Decade (Turow et al, 2015)

- Summary The article sets forth the existence of a disconnect between what consumers believe "privacy policy" means and what the term actually means. Consumer associate the term "privacy policy" with practices to afford *them* protections, while the article opines that the FTC should regulate the term to ensure that companies deliver a set of protections so as to not mislead consumers. The article cites surveys that indicate consumers care deeply about privacy, but misunderstand online data collection and its rules in the marketplace. According to the studies cited by the article, although most consumers correctly identified that websites may retain their information, they incorrectly believe that privacy policies prevent the sale of their information. Further, consumers who cannot understand the agreements may unwittingly install malicious spyware or viruses, so the FTC should step in to protect consumers by providing clear, understandable information. The article opines that the solution is threefold: 1) the FTC should police the term "privacy policy," 2) privacy mechanisms should be vetted by experts, and 3) the FTC should set benchmarks for self-regulation.
- Your opinion of the article: This article goes to to the core of the problem: when consumers do not understand, they are under mistaken impressions and are unable to make an informed choice of deciding whether to prefer free/ad-supported products or non free nor ad-supported products.

  Author/Affiliation/Contact information: JOSEPH TUROW, CHRIS JAY HOOFNAGLE, DEIRDRE K. MULLIGAN, NATHANIEL GOOD, & JENS GROSSKLAGS, The Federal Trade Commission and Consumer Privacy in the Coming Decade, 3:3 I/S: A JOURNAL OF LAW AND POLICY 723, (2008). Joseph Turow, Ph.D., Annenberg School For Communication University of Pennsylvania Philadelphia, PA https://www.ntia.doc.gov/files/ntia/comments/100402174-0175-01/attachments/FTC_and_privacy.pdf

3. Paying for Privacy and the Personal Data Economy (Elvy, 2017)

- Summary: This article explores emerging trends in the personal data economy, where companies purchase data directly from consumers. Additionally, the article explores the "pay for privacy" model which requires consumers to pay an additional fee to prevent their data from being collected and mined for advertising purposes. The article identifies a typology of data-business models, and it uncovers the similarities and tensions between a data market controlled by established companies that have historically collected and mined consumer data for their primary benefit and one in which consumers play a central role in monetizing their own data. The Article makes three claims. First, it contends that PFP models facilitate the transformation of privacy into a tradable product, may engender or worsen unequal access to privacy, and could further enable predatory and discriminatory behavior. Second, while the PDE may allow consumers to regain a semblance of control over their information by enabling them to decide when and with whom to share their data, consumers' direct transfer or disclosure of personal data to companies for a price or personalized deals creates challenges similar to those found in the PFP context and generates additional concerns associated with innovative monetization techniques. Third, existing

frameworks and proposals may not sufficiently ameliorate these concerns. The Article concludes by offering a path forward.

- Opinion of the Article: This is a great article that details current PFP and PDE models and their implications for the future as technology and new sources of valuable data proliferate (including the impact of data-sharing in the IoT era). The article goes on to further articulate how the disparities created by these data sharing models could lead to discriminatory or predatory practices.
- Citation: Stacy-Ann Elvy, Paying for Privacy and the Personal Data Economy, 117 Colum. L. Rev. 1369 (2017)
  Contact: Stacy-Ann Elvy, Professor of Law, New York Law School

**Responses to 4d**

the benefits and costs of privacy laws and regulations, including the effect of such regulations on innovation, product offerings, and other dimensions of competition and consumer protection

1. Never Home Alone: Data Privacy Regulation for the Internet of Things (Ly, 2017)

- Summary A rigid regulatory approach to the nascent IoT industry poses potential risks to consumers, but the current free-market approach to data privacy has already proven to be harmful. Overregulation might stifle innovation for the sake of eliminating relatively remote risks, and in turn eliminate legitimately advantageous technology. Overregulation would also likely create anti-competitive market conditions, including: higher costs, lower quality, and a more limited range of product choices. Any overly strict regulation would be premised on a series of flawed assumptions, including: that the government knows what types of data should or should not be collected, that the government understands manifestation of consent in a fast-paced, digitally-enhanced environment, and perhaps most troubling, that the government is able to predict how companies might use consumer data in the future. However, the potential harms to consumers stemming from data collection and use are not negligible. The current status of the market, with a lack of regulation and a deep lack of understanding of IoT technology provides fertile ground for corporate exploitation of consumer data. There is a general sense of apprehension amongst consumers and tech professionals alike that data on our devices is not secure. We need general data privacy regulation that mandates best practices and outlines use restrictions flexibly, because we cannot rely on the assumption that the full range of potential harm can be determined in advance. The FTC's strategy to-date of nudging encouragement of use restriction is inadequate because it relies on corporations for self-enforcement.
- Opinion: Ly provides an overview that outlines the relative advantages and tradeoffs of three schools of thought on data privacy regulation: the free market camp, the activist camp, and the FTC's approach to date (as of Fall 2017). Ly perhaps relies too heavily on the premise that the FTC's Section 5 enforcement authority is sufficient to deter harmful corporate data collection and use practices.
- Author/Affiliation/Contact Information: Ly, Branden, "Never Home Alone: Data Privacy Regulations for the Internet of Things" (2017). Journal of Law, Technology & Policy, University of Illinois College of Law. Vol. 2017 No. 2.
  http://illinoisjltp.com/journal/wp-content/uploads/2017/12/Ly.pdf. Journal of Law, Technology & Policy University of Illinois College of Law

2. IoT and Wearable Technology: Privacy vs Innovation, 1-53, 60-78 (Thierer, 2015)

- Summary The internet of things market is expanding rapidly. There's so much potential to make life better and for big data to have a part in it. Health app use is on the rise. It's up to consumers and inventors to decide what products will succeed. This article will focus on wearable tech such as fitbits and body cameras.
- There are two opposing thoughts on policy, permissionless innovation and precautionary principle. The precautionary principle supports strict regulation requiring innovations to prove they don't cause harm before being allowed to enter the market. The point is the get ahead of new

technology before it causes harm. Permissionless innovation supports new technology and business models being allowed to enter the market by default with any regulation coming only after proof of harm. The point is that the benefit of some technologies takes time to discover. The precautionary principle does not allow the best case scenario since it always guards against the worst case scenario. It also raises the cost of entering into a market, raises the cost of goods and services, diminishes the quality of those goods and services, and limits the range of choices in the market. Resisting the urge to plan for every possible outcome allows the consumers to make choices about what they want. Since technology evolves faster than law, educated policy makers are key. A consent model can be difficult in a world where companies can collect data through others. A move towards use restrictions could solve this problem, but would not silence all concerns about the collection of sensitive data. Broad restriction in this case could limit helpful innovations. Consumers have the right to trade off sharing information for free ad-based apps. Good practice for companies would include providing users with information, transparent data use, and limited use and retention. A layered approach is best since there's no one size solution.

- The First Amendment could restrict regulation. People recording video and audio is an important part of people having the right to distribute those recordings. Regulators need to narrowly tailor measure to avoid First Amendment complications.
- Your opinion The article does a good job of discussing policy rationale even though it mentions google glasses frequently. An important note is that the First Amendment frequently outweighs privacy concerns.
- Adam Thierer, The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation, 21 RICH. J.L. & TECH. 6 (2015), http://jolt.richmond.edu/v21i2/article6.pdf.

3. Competition, Consumer Protection, and the Right (Approach) to Privacy (Ohlhausen et al 2015)
   - Summary: The Article explores the use of competition law to address privacy concerns by examining the historical development of privacy protections in the US. The article traces the historical development of privacy protections in the US to the advent of the portable camera and subsequent recognition of a legal right to privacy under tort law and eventual development of codified privacy law. The proliferation of computer and communications technology led to the development of additional affirmative privacy protections i(i.e. the Fair Credit Reporting Act). With the widespread use of the internet beginning in the 1990s, an individual's information is now more accessible and more commercially valuable than ever before. Based on the FTC's traditional approach to competition and consumer protection, the Article concludes that these fields are complementary, but should not commingle - competition is about economic efficiency while consumer protection is about harm to individuals. To that end, fitting privacy concerns into competition/antitrust law, in many cases, requires difficult contortions of antitrust law and a consideration of many factors remote from economic efficiency. This is bad for the protection of privacy and adjudication of non-privacy related antitrust issues. The better avenue is to protect privacy through the FTC's consumer protection powers as it better encapsulates the type of harm, scope of harm, and remedies to harm.
   - Opinion of the article: An interesting overview of the legal history of privacy law and the FTC's authority to remedy privacy violations. The Articles raises good points about the differing purposes of competition and consumer protection law and supports its conclusion that competition law represents an unnecessary and oftentimes inapplicable remedy to privacy violations.
   - Citation/Author/Affiliation/Contact information: Ohlhausen, Maureen K. and Okuliar, Alexander, Competition, Consumer Protection, and the Right (Approach) to Privacy (February 6, 2015). Antitrust Law Journal, Forthcoming. Available at SSRN: https://ssrn.com/abstract=2561563. Maureen K. Ohlhausen, Federal Trade Commission Commissioner. 600 Pennsylvania Avenue, NW Washington, DC 20580 United States. Alexander Okuliar, Orrick, Herrington & Sutcliffe, LLP.

4. Privacy, mHealth and HIPPA (Addonizio, 2015)
   - Summary: The article discusses privacy risk associated with mobile health ("mHealth") and fitness apps, and corresponding wearable devices: including collection of personal sensitive information without consent, sharing private health and non-health related information with third parties, undeveloped or non-transparent privacy policies, and unsecured data transmission. It summarizes how personal information is being collected, stored, used and shared, e.g., for analytic services and advertising purposes. The author emphasizes that consumers often give away such information without consent or even noticing it. The article sets forth the gap between technology innovation and policy and regulation.While HIPAA's Privacy Rule protects the use and disclosure of individuals' "protected health information" ("PHI"), it is limited to covered entities and its business associates. Put simply, when there is no covered entity or business associates involved in the usage, transmission, management and storage, mHealth apps do not need to be HIPAA compliant. While the FTC Act safeguards consumer's data by going after app developers for unfair acts and deceiving practices, it does not prevent the sale of PHI nor does it require health apps to obtain consent for use and disclosure of information. Lastly, the author suggests that app developers and wearable device designers take preemptive actions to ensure consumers' privacy is protected: initiate self-regulation through its transparent privacy policy, disclosure and notification of leaks, sharing and data transmission to third parties.
   - Your opinion of the article: This article highlights the central issue of technology, regulation and consumer expectation. The author describes the intricacies of fast development of technology and the lag of corresponding policy /regulation, and its impact on consumer privacy risk. The author provides insight into how misperception or lack of understanding of the law lead consumers to put their confidence in the legal system assuming that their privacy is protected, without considering the privacy risk they are compromising.
   - Author/Affiliation/Contact information: Addonizio, Gabrielle, "The Privacy Risks Surrounding Consumer Health and Fitness Apps, Associated Wearable Devices, and HIPAA's Limitations" (2017). Law School Student Scholarship. Paper 861. http://scholarship.shu.edu/student_scholarship/861

5. The Privacy-Innovation Conundrum, ICT Industry
   - Summary: The article discusses the interplay between privacy laws and regulations and innovation. The article does so through the lens of privacy laws and regulations in the United States and European Union and the state of innovation in those 2 geographical arenas. The article, published in 2015, is written with an eye toward the then soon-to-be-passed General Data Protection Regulation, which has now been in effect for almost 3 months. The general leniency of U.S. privacy laws and regulations and strictness of E.U. privacy laws and regulations sets the stage for the article's privacy v. innovation discussion. The article presents the idea that the U.S.-centric argument that privacy laws and regulations inhibit innovation may be a manipulative tool to forestall more restrictive privacy laws and regulations, and even that the argument can be "wrong" and "offensive." Another idea presented in the article is that based on the disparities between innovation in the two arenas, the aforementioned U.S.-centric argument may have some merit. In making that latter point, Professor Zarsky discusses, in a more empirical tone, the relation between U.S. companies' success in the internet/information and communication technology space and lenient U.S. privacy laws and regulations, as well as the counterexample of such companies' less successful ventures in the internet space in the E.U. Ultimately, the author states that the U.S.-centric argument may be more beneficial than the E.U.-centric argument due to the author's belief in the importance of innovation in the ICT space due to such innovation's democratizing abilities and fostering of free speech.
   - Opinion of the article: The article is a provocative assessment of the U.S. v. E.U. privacy-innovation debate. While stating that adopting the radical end of the U.S.-centric argument is a path replete with concerted manipulation, Professor Zarsky states there does seem to be merit to the broader U.S.-centric argument in that it creates an innovation-friendly environment, which ultimately has a democratizing dimension to it.
   - Citation/Link/Author/Affiliation/Contact information: Zarsky, Tal Z., "The Privacy-Innovation

Conundrum" (2015). 19 Lewis & Clark L. Rev. 115. Prof. Tal Z. Zarsky, University of Haifa,

6. Artificial Intelligence and Consumer Privacy
   - Responsive to 4d: The benefits and costs of privacy laws and regulations, including the effect of such regulations on innovation, product offerings, and other dimensions of competition and consumer protection
   - Summary: The article discusses the consumer privacy in light of "big data" and artificial intelligence. It highlights the risks of data theft and consumer privacy. The article also discusses consumer attitude, surveys clearly bring out a "privacy paradox". While consumers are aware of the risk involved, they are ready to give away information in exchange for freebies etc. The article also discusses the steps big data companies have taken to protect consumer privacy. The article also discusses the current law and policy landscape such as state and federal laws that currently industry specific. At the state level 48 out of 50 states have a enacted data breach notification laws, however, there is an ongoing debate on a need for a federal law on data privacy. The article offers solutions to data and privacy breaches due to AI, including defining and including privacy and data use as a right , as done under the new GDPR which recognized individual rights of data access, data processing, data rectification and data erasure.
   - Opinion of the article: Big data and AI in general are rapidly becoming an integral part of modern life, consumers need to be more aware of their privacy rights. There are several state laws, individual federal laws, as well as the FTC already in place to protect consumer privacy, but is this enough? Companies that handle big data are not quite ready to take the onus of data protection. There is a need for further laws and rights to consumers that can have a bigger impact on data privacy and consumer rights, whilst not stifling the economy or innovation.
   - Citation/Link/Author/Affiliation/Contact information of the author: Ginger Zhe Jin, ARTIFICIAL INTELLIGENCE AND CONSUMER PRIVACY, NBER WORKING PAPER SERIES(2018). University of Maryland and National Bureau of Economic Research,

7. Privacy and Big Data: Making Ends Meet
   - Responsive to question 4(d), "the benefits and costs of privacy laws and regulations."
   - This article is not one that provides a clear-cut answer to the questions of privacy and big data - indeed, it claims that to do so would be pretentious. Instead, it offers a perspective that a more narrowly-focused piece would perhaps lack, suggesting that the benefits and drawbacks of big data must be considered *as they fit into the overarching priorities and standards of a given culture.* The article makes the case for these benefits being considered separately for each place they may be found, before attempting to assess them within the framework of privacy regulation. One of the most interesting points this piece makes is that the utility of big data depends not on an absolute value, but on the probability that said a given benefit or cost will arise. It uses this point to further the "cultural situation" argument briefly detailed above, pointing out that America - at least in its own eyes - is the land of the pioneer, and the lone explorer, and therefore expresses a more unfettered view of data use.
   - I believe this article is exceedingly useful, as it demonstrates the need for a broad-context view of such issues. It is very rare, when dealing with emergent technology, that a one-size-fits-all approach will work, and this article is a good starting point to appreciate such issues. This takes a practical, realistic view of a field all too often sensationalized and preached on from on high. While it is an older piece, the same concerns remain present today.
   - Polonetsky, Jules and Tene, Omer, Privacy and Big Data: Making Ends Meet (September 3, 2013). Stanford Law Review, Vol. 66, No. 25, 2013. Available at SSRN: https://ssrn.com/abstract=2628412

8. Privacy and Innovation

Summary: The article discusses the potential implications of privacy regulations on innovation and argues that digitization has made privacy policy a part of innovation policy. The authors provide an overview on how companies are using personal data and gives examples of specific use-cases and sector-specific uses. For example, the article discusses personal data collection in health care and provides examples of how data is used to improve operations of a business.

- Your opinion of the article: I found the article to be informative and well organized. I was particularly interested in the section that discussed the effect of privacy regulation on health care provider's likelihood of adopting new technologies. Having worked on the business side of several tech companies that engage with health care providers, I have seen first-hand how these organizations are hesitant to adopt data storage and processing technologies due to concerns of remaining compliant with data privacy regulations.
- Citation/Link/Author/Affiliation/Contact information of the author: Avi Goldfarb and Catherine Tucker, "Privacy and Innovation," *Innovation Policy and the Economy* 12 (2012): 65-90.

9. The Impact of the EU General Data Protection Regulation on Scientific Research
   - Summary: The Article discusses the impact of the EU's General Data Protection Regulation ("GDPR") to scientific research involing the use of large amounts of personal data. The GDPR forbids the processing of certain types of data, most notably "Data Concerning Health" and "Genetic Information," except for research purposes and archiving the public interest. However, even in within the research exception, the GDRP implemented additional requirements and mandatory safeguards for the use of personal data. Most personal data that could be used to identify the research participants needs to be protected by encryption, reducing the risk caused by data breaches. A Data Protection Officer ("DPO"), who must be an expert on the field and the law, needs to be kept on hand to advise the research firms how to comply with the GDPR with every proposed use of data, although the DPO is only an "initial expense." Research firms need to inform everyone involved of potential data breaches unless the data was protected via encryption. Research firms need very specific forms of consent for the. Finally, the research firms usually must seek new consent from the subject if they wish to reuse any previously obtained data for different lines of research, although there is an exception for certain scientific research where it is unclear from the outset how the data would be used in the study. The article concludes that the GDRP strikes a balance between protecting people's data and the usability of that data for research.
   - Your opinion of the article: The article does not go into specific costs of complying with the GDPR or the potential for on less well-funded research being canceled due to the additional expense. The article also considers the DPO as an initial cost rather than a continuing cost, even though the Officer is an employee that needs to be informed and consulted throughout the entire research process. The article also does not suggest how the new consent requirements will impact double blind research and studies, where the need to keep how the data usage secret from the subject. In sum, the article does not thoroughly discuss the potential negatives of the GDRP on research.
   - Citation/Author/Affiliation/Contact information: The Impact of the EU General Data Protection Regulation on Scientific Research, By Gauthier Chassang , published January 3, 2017. retrieved from US National Library of Medicine National Institutes of Health: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5243137/

**Responses to 4e**

the benefits and costs of varying state, federal, and international privacy laws and regulations, including conflicts associated with those standards.

1. Article: The Privacy Policymaking of State Attorneys General. 92 Notre Dame L. Rev. 747 ,

Danielle Citron

- Summary: This article takes a deep dive into the role state attorneys general take in enforcing privacy laws in their individual states, given their ability to drive their own policies and standards. The article mostly praises the fact that there are varying requirements from state to state regarding privacy regulations, stating in part that this system is efficient because of state by state specialization and aggressive enforcement by individuals who are usually ambitious. It highlights the fact that state AG offices have specialized in consumer protection issues that are unique to their state and can cooperate with other states in those areas (California for example has developed a speciality in regulating privacy within big tech, whereas New York has done so in the realm of big finance). The article also discusses the that some of these stronger state laws could and should be passed by congress if they are strong on consumer protection, to create a national standard for certain privacy policies such as data breach notification. However in place of this the article also talks about the strong pull of the "California Effect" within privacy law enforcement, which describes a phenomenon in which companies comply with the strictest state laws as a matter of internal policy to avoid conflicts with the large markets of states.
- Opinion of the Article: It is a lengthy read, but it provides a very helpful and detailed walkthrough of the role individual state attorneys general play in the creation and enforcement of privacy policies. The article is very strongly in favor of the power of individual state AGs enforcing policy and describes the benefits of this. However, this article does come off as a bit of a laundry list of accomplishments from individual AG offices instead of a proposal of policy. The main takeaway is that state AGs are very effective policy shops for federal public policy and there is a legitimate argument that strong consumer protections in areas such as data breach notification could go federal (since all 50 states have different requirements).
- ARTICLE: The Privacy Policymaking of State Attorneys General. 92 Notre Dame L. Rev. 747
  Author: Danielle Keats Citron |

Responses to 4f

competition and consumer protection implications of use and location tracking mechanisms."

1. Mobile Privacy: A User's Perspective, FTC v. Snapchat, FTC v. Brightest Flashlight Free

- Summary: Studies find that significant majority of users (77%) do not wish to share their location data with app owners or developers. Nine out of ten users would not be willing to share photos, contact list, or surfing behavior even in exchange for money.
- Despite regarding privacy as heavily important, more than half of smartphone users do not read or understand privacy policies of mobile applications.
    - 56% of users are concerned that their information is shared with others without permission
    - 52% of users are concerned that their information will be shared with or without their permission
    - 51% of users are concerned their info will be used to identify them
    - 51% of users are concerned that virus or spyware will be installed on their phone
    - Nearly three-quarters of consumers are uncomfortable with the idea of advertiser tracking, and 85% want to be able to opt into or out of targeted mobile ads
    - Opinion of the article: Very informative and large amounts of data regarding consumer behavior and preferences.
    - Author Affiliation/Contact Information: Harris Interactive, "Mobile Privacy: A User's Perspective", 2010. Retrieved from: https://www.scribd.com/document/54220855/TRUSTe-Mobile-Privacy-Report?doc_id=54220855&download=true&order=449157922
    - FTC has issued complaints against Snapchat, Brightest Flashlight Free Application, and other companies for deceptive and misleading privacy disclosures and practice.

- From June 2011 to February 2013, Snapchat's privacy policy stated, "We do not ask for, track, or access any location-specific information from your device at any time while you are using the Snapchat application."
- In October 2012, Snapchat integrated and utilized an analytics tracking service in the Android version of its application, without disclosing the integration to users.
- Consumers could not ever prevent Brightest Flashlight App from collecting or using their device data.
- Although consumers expected the application to not function without users agreeing to the application's user agreement, Brightest Flashlight App transmitted user's device data before users ever agreed to the End User License Agreement.
- Brightest Flashlight App did not disclose to consumers that the app transmits device data, including precise geolocation along with persistent device identifiers to third parties, including advertising networks.

2. Track Me Maybe: The Fourth Amendment and the Use of Cell Phone Tracking to Facilitate Arrest
   - Summary: Starting from Fourth Amendment basics, the article concludes that cell phone tracking is acceptable to aid in the arrest of a suspect, but not in the pursuit of evidence of criminal behavior. The author begins with surprising statistics. Specifically, the author cites the 20-30k tracking requests in the federal court system alone (in 2011) and the rapid increase in the precision of such tracking, from hundreds of feet to a few yards in the span of four years. The author reviews the main types of tracking mechanisms used by the police historical cell-site location information (CSLI), real-time CSLI, and GPS. The author then reviews the basics of Fourth Amendment search jurisprudence with respect to using electronic devices to track people. The most interesting part of the article pertains to the "Third Party Doctrine," which says a person who voluntarily gives up information to a third party cannot expect that information to be protected by the Fourth Amendment. Though initially courts seemed to have said cell-phone users could not expect to realize their position information is broadcast every time they make a call or send a text, it appears more recent cases disagree, at least with historical records of imprecise CSLI tracking. For modern precise tracking, no cases are on point. Relying on *N.Y. v. Payton,* the author concludes that using precise location information to assist in an arrest is analogous to a home search, but a precise search for investigative purposes under the same reasoning is not proper.
   - The article provides a great starting point for any conversation about cell-phone location tracking as it pertains to criminal investigations.
   - Citation/Link/Author/Affiliation/Contact information: Rothstein, Jeremey H., "Track Me Maybe: The Fourth Amendment and the Use of Cell Phone Tracking to Facilitate Arrest" (2012). Fordham Law Review. Vol. 81, Issue 1, Article 9. Link. Email:

3. BETTER KEEP YOUR HANDS ON THE WHEEL IN THAT AUTONOMOUS CAR: EXAMINING SOCIETY'S NEED TO NAVIGATE THE CYBERSECURITY ROADBLOCKS FOR INTELLIGENT VEHICLES
   - Summary: This article discusses a wide array of issues related to the privacy and security of autonomous vehicle. First, the article addresses the state of the law regarding autonomous vehicles and points out that we are dealing with two distinct area of law: computer and vehicle. Second, the article discusses inherent weakness of autonomous vehicles to hackers and invasion of privacy. The nature of autonomous vehicles will be that they "talk" to nearby cars to maximize efficiency, yet at the same time not too much of the driver's information can be leaked to threaten his or her privacy. Finally, the article concludes with an analysis of the current state of the law. Concerns that must be addressed include vehicle hackers, licensure of drivers, and the use of data reviewed by manufacturers regarding their systems must be addressed.
   - Opinion of the Article: This article raised many fascinating issues that I had not considered. The

nature of big-data will allow every move we make be tracked by car/ autonomous system manufacturers at all times. These systems will need to be closely monitored to ensure our privacy and will likely require an entirely new scheme of regulations that combines CFAA/DMCA with vehicle laws. Location tracking mechanisms could be exploited by systems manufacturers in ways that threaten our 4th amendment. Further, drivers should also concerned about passing information to other drivers, as vehicle-to-vehicle communication will be an essential component to autonomous vehicle. During such information transfers, driving systems may be vulnerable to hacking. Thus, there is an immediate need to pre-empt autonomous vehicles with proper regulation.

- NOTE: NOTE: BETTER KEEP YOUR HANDS ON THE WHEEL IN THAT AUTONOMOUS CAR: EXAMINING SOCIETY'S NEED TO NAVIGATE THE CYBERSECURITY ROADBLOCKS FOR INTELLIGENT VEHICLES, 45 Hofstra L. Rev. 707
- Contact Information: Christopher Wing,

4. Location-Sharing Technologies: Privacy Risks and Controls; Protecting Privacy in Continuous Location Tracking Applications
   - Summary:
     - an online survey of American Internet users (n = 587) to evaluate users' perceptions of the likelihood of several location-sharing use scenarios
     - Survey of magnitude of the benefit or harm of each scenario (e.g. being stalked or finding people in an emergency)
     - Result: Although majority of our respondents had heard of location-sharing technologies (72.4%), they do not yet understand the potential value of these applications. Overall, respondents feel the risks of using location-sharing technologies outweigh the benefits. Most likely harms concerned: revealing the location of their home to others or being stalked. Benefit: being able to find people in an emergency and being able to track their children.
     - Survey on existing commercial location-sharing applications' privacy controls (n = 89): location-sharing applications do not offer their users a diverse set of rules to control the disclosure of their location, they offer a modicum of privacy
   - Opinion of the article: This is a very empirical article based on hundreds of survey results. By defining the relative value of users' expected risks and benefits regarding the use of location sharing services, the author recommends location-sharing applications consider making more expressive privacy controls available to their users.It articulates users' concern in a way that guides the policy.
   - Citation/Author/Affiliation/Contact information: Janice Y. Tsai, Patrick Gage Kelley, Lorrie Faith Cranor, Norman Sadeh Carnegie Mellon University Pittsburgh, PA

     Updated February 2010

5. Privacy Issues in Location-Aware Mobile Devices; Third-Party Web Tracking: Policy and Technology
   - Summary The *first article* gives an overview of what location-aware devices are and how they can track location through either internal or external means and the information used, disclosed, or stored by the collector. The articles tries to balance with good and the bad by bringing up positive things about location tracking such as targeted retail ads and safety of children. The article then enumerates thirteen privacy issues that arise, including the type and length of stored information, the competitive advantage location-tracking provides companies, and the level of regulation on disclosing of collected information with third-party vendors. The article is older, so it mostly serves as explanatory research.The *second article* provides first an explanation of what tracking information is available to third-parties, then discusses how this could be potentially harmful and lastly discusses survey results where consumers repeatedly say that they prefer not to be tracked. The article finds connections between browser history (which is easily tracked) and personal information and how third parties obtain access to such information when their

information is displayed on a website that collects information (such as browsing history or location tracking).

- Your opinion The first article was a good overview of the development of location tracking and the second article provided more context as to how it is used. I liked that the articles tried to present the concerns in a way that doesn't cause mass panic - presenting positives and negatives within the same portions of the articles. I think this is a much better way of presenting the concerns.
- Citation/Link/Author/Affiliation/Contact information: 1) Robert Minch , Privacy Issues in Location-Aware Mobile Devices, Proceedings of the 37th Hawaii International Conference on System Sciences, IEEE (2004) 2) Jonathan R. Mayer and John C. Mitchell , Third-Party Web Tracking: Policy and Technology, IEEE Symposium on Security and Privacy (2012)