The Impacts of Data and Informational Privacy on Consumer Trust and Behavior

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Bryce Huffman

Spring, 2022

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Advisor

Bryn E. Seabrook, Department of Engineering and Society

The Explosion of Digital Technologies and Personal Data

Masked beneath each click, tap, or scroll that an individual makes with a digital technology, such as social media or other online-based platforms, is a multifaceted universe with copious amounts of personal data. This trove of data is primarily derived from the user's interactions with the technology using complex methods, often unbeknownst to the user. The rise in personal digital technologies and their respective growing entanglement with society has ushered in the era of big data (Cooke, 2008). Big data refers to the massive increase in data collection and availability within the technological sector that is predominantly sourced through individual's interactions with platforms (World Economic Forum, 2012). These technologies continue to rapidly accelerate in development, deployment, and adoption, thus leading to expanded potential for personal data collection opportunities (Balaban and Mustățea, 2021). According to the United Nations (2021), this phenomenon is critically urgent as digital technologies have "advanced more rapidly than any innovation in our history – reaching around 50 percent of the developing world's population in only two decades" (para. 1). Understanding the complexities of personal data through the lens of consumer trust and behavior is paramount to enabling understanding of how to develop technologies from a user-centered design approach. In particular, such design theory frames all decisions through the lens of end-user needs. This approach for technology development is not only productive but also responsible as many digital platforms are practically unavoidable throughout one's day. Approaching technological development from a user-centered design ideology facilitates the ability for user's data and interconnections to be discussed, understood, and developed for the benefit and protection of the user.

This analysis aims to understand what implications data privacy practices, whether in actuality or perception, have on consumer trust and behavior for a typical end-user, or personal customer, within the United States of America. Actor-network theory, often abbreviated to ANT, is primarily employed to unearth the underlying, complex sociotechnical systems that stem from personal data collection and use. Viewing the multiplex data privacy system through actor-network theory enables each actor or agent and their associated web of translations, or interconnections, to be examined in a comprehensive model.

Discourse Analysis of Personal Data Privacy Actor-Networks

The research question of understanding how data privacy practices influence consumer trust and behavior is addressed through discourse analysis, via a comprehensive literature review, followed by a sociotechnical synthesis that is reliant upon the actor-network theory sociotechnical framework. Keywords of data privacy, perception, trust, actor-network theory, and consumer behavior identify scholarly literature and subject-matter expert content. This conglomerate of research is synthesized to establish an understanding of the descriptive, or current, personal data privacy situation, what actors exist within the system in scope, and how such actors associate with one other thus forming actor-networks. While extensive, this research methodology approach fulfills inquiry demands to adequately map the complex web of connections between all players, or actors, within the personal data privacy apparatus; without such information, it would be implausible to examine the implications of such structures on consumer trust and behavior.

The Evolving Tenets of Data Privacy

Privacy has no single definition but rather exists as a heterogenous makeup of ideologies amongst scholars and subject-matter experts. As referenced in research by Louise Cooke (2008),

a professor of information and knowledge management at Loughborough University, privacy was historically "understood as concerning itself with notions such as secrecy, solitude, security and confidentiality" (p. 167). However, with the rise of big data, a novel framework of privacy, coined as informational privacy, was explained by Luciano Floridi (2005), a professor of Philosophy and Ethics of Information at the University of Oxford, as relating to the extent to which third-parties have access to an individual's personal data and information. The idea of informational privacy was again echoed by privacy researchers who asserted privacy is "the state of being free from public attention" (Cohen et al, 2020, p. 4). The definition of privacy has evolved over time with the changing state of technological development.

Relying on the notion of informational privacy enables each technological advancement within the era of big data to be viewed from the perspective of how prohibitive it is for others, whether unauthorized or authorized, to obtain data on an individual. Within this analysis, any reference to privacy utilizes this concept of informational privacy. It is critical to focus not only on those who gain unauthorized access but also on those who possess authorized access to an individual's data; unauthorized access carries the same, if not greater, risks to users. Due to government regulations, most products and services require users to agree to a terms and conditions or privacy policy prior to using the respective technologies. However, as explained by communications professors Jonathan Obar and Anne Oeldorf-Hirsch (2020), customers often accept usage terms and conditions or privacy policies without much examination of the documents. They described this observation with the paradox of "when asked, individuals appear to value privacy, but when behaviors are examined, individual actions suggest that privacy is not a high priority" (p. 22). Furthermore, this aligns with the results of a North American survey that found, "87 percent [of customers] – said they would not do business with a company if it gave

away sensitive data without permission" (Anant et al, 2020, para. 1). Consumers of digital technologies often grant access to data without considering the potential risks. The plurality in the definition of privacy in terms of consumer data combined with the paradoxical elements of individual behavior bring relevance and urgency to the issue of data privacy and the internalized fostered trust.

Although the issue of informational data privacy should take a customer or user-centric approach, that does not necessitate a mutually exclusive benefit to any sole party. As detailed by psychology researcher Edward Wang (2019), any lack of positive consumer perception in a firm's privacy practices can lead "to losses for online businesses and exerting a considerable negative effect on online business performance" (p. 60). Although Wang strictly mentions online business, their idea should apply to traditional, in-person firm interactions as most, if not all, entities have an underlying online presence. For example, in an opinion piece for the New York Times, Michael Kwet (2019), a visiting fellow at the Information Society Project at Yale Law School, brings awareness to the level of surveillance that often occurs in a physical store without awareness of the customer. Kwet notes how Bluetooth beacon sensors are often placed throughout stores to collect data on customers by using their personal devices without consent. Therefore, the notion that one can entirely escape the virtues of online data collection is practically mistaken. To restrict the issue of data privacy regarding customer trust and perception to online-only platforms would be short-sighted and inadequately scrutinize the society of big data and technologic innovation that exists today and continues to advance.

Under the aforementioned notion of informational privacy, the actors that compose the system of actor-networks emerge. From a top-down hierarchical perspective, the following actors are the most significant, defined in terms of prevalence and influence: personal

consumers, government legislation and legal precedents, capitalist firms, and personal computing hardware or technologies. Without any one of these aforementioned actors, any actor-network model would fail to encapsulate the forces, or translations, that shape the subject. Each actor could be subset into numerous components but not without risks of increasing the network complexity to such a level that renders the overarching relationships trivial.

Actor-Network Theory

Actor-network theory is a sociotechnical, or STS, framework that uses the identification and study of all actors with a network or system through intermediaries and translations (Cressman, 2009). In ANT, actors are any entity that is involved in the system while a network is any interconnected relationship between multiple entities. Furthermore, intermediaries are fundamental linking mechanisms that bridge communication between actors while translations are the instruments that provide structure and meaning between actors.

As explained by David Cressman (2009), an STS scholar at Maastricht University, each inclusion in the framework is considered both an actor and a network as "an actor-network is simultaneously an actor whose activity is networking heterogeneous elements and a network that is able to redefine and transform what it is made of" (p. 3). Although complex, viewing each actor as a network in the context of consumer trust and behavior in regard to data privacy enables the unveiling of explanatory linkages. This methodology allows for the black box phenomena of complex interconnections between the technical and social elements of the actor-networks to be examined then analyzed.

Previously, actor-network theory has been utilized by scholars across disciplines in a slew of applications. In one case, ANT was integrated through a historical lens to contextualize the development of freedom of information, often known as FIP, and freedom of information and

protection of privacy, often known as FOIP, memoranda across the globe (Bronner, 2013). This application involved data privacy policies pertaining to government records of vehicle ownership from the 1990s to the early 21st century. Additionally, actor-network theory was utilized to examine how airport scanning and security systems can be approached in design by developing a heterogeneous model that has specific technologic arrangements (Valkenburg & van der Ploeg, 2015). Lastly, actor-networks were mapped to understand how design of daily objects and environments, such as lecture halls, influences human behavior (Yaneva, 2009). None of these applications directly contain learnings that coincide with the scope of this analysis but rather show the viability of using ANT in a nearby field. This analysis of consumer trust and behavior relating to data privacy practices represents new contributions to the existing sociotechnical scholarly knowledge.

The widespread use and flexible applications that actor-network theory affords does not exclude it from criticism. Most criticism of ANT center around the minimization of pre-existing social structures and hierarchies as all actors, human and material, are viewed from an equal footing (Modell, 2020). Although there exist potential shortcomings of ANT, it remains valuable to explain the interactions between webs of actors. Viewing the issues of consumer trust and behavior from data privacy has no single path, however, actor-network theory will enable a comprehensive analysis and thoughtful understanding.

From a simplistic vantage point, no single actor in the system of data privacy can exist or be modified without exerting influence on at least one other actor within the network. This fundamental idea is the driving force behind why actor-network theory is well-suited for this particular analysis. Moreover, a simpler, more linear framework would be inadequate for this

application as the agents involved in the data privacy and consumer trust realm create a dense mesh of interconnections.

The Entanglement of Consumer Trust and Behavior within Data Privacy

An individual's concerns with digital platforms or services informational data privacy practices lead to diminished trust and altered behavior. Although the magnitude of each consumer's behavioral shift varies, the impacts consistently trend in a negative direction; higher levels of concern lead to decreasing levels of trust and a reduction in the usage level of the service. Within the sphere of personal data, each actor has different, and often conflicting, motives, desires, and overarching goals. Most, but not all firms, who are viewed to hold the most concentrated power and influence, lean towards weaker privacy policies to bolster revenues and profits. On the contrary, consumer preferences tilt towards more cautious approaches regarding the collection and use of their personal data. By prioritizing user-centered design objectives, platforms can be designed, and regulation can be devised, with trust at their cores thus providing positive consumer behavioral patterns.

Fundamental to the notion of privacy, all personal data that exists today was at one point derived from a consumer whether by explicit consent, surveillance collection practices, or via third-party sources (Goddard, 2019). However, the overarching purpose that any for-profit firm has in such data access is the desire to use personal data to drive analytics to generate more revenue, reduce operating expenses, and thus increase profits ("Your data is," 2019). Although firms may market the use of data for the sole benefit of the consumer, there are often ulterior motives to such practices. For instance, while a firm may utilize user data to create a curated playlist for a user, they likely have additional motives of establishing user loyalty to the provided service to increase revenue. This need not imply that all use of data by firms is always malicious

but rather the purpose for data collection is often layered and complex. With the aforementioned information, each firm that is involved in such practices is an actor within the data privacy actor-network. While these for-profit firms vary in low-level characteristics and missions, all can be considered in one consolidated actor as their high-level objectives and interactions remain relatively constant.

Consumers have differing levels of awareness and knowledge regarding information and data collection and privacy practices (Auxier et al., 2019). Regardless of their expertise relating to their own data privacy, most consumers, when surveyed, are willing to exchange personal data for tailored services that provide a net positive benefit (Gothmann, 2021). This finding does not imply that consumers will share or unknowingly give up any amount of personal data that another party desires as long as any level of benefit is promised in return. Notably, the proportion of consumers who have concerns about their personal data is increasing, now reaching nearly eight out of every ten individuals (Gothmann, 2021). Quantifying such trade-offs between tailored services and data privacy is complex and ill-defined, but acknowledging such phenomena indicates that consumers often do not have a preference that is strictly binary. Although assuming that the behavior of each consumer is identical would be shortsighted and inaccurate, aggregating consumer behavioral patterns and shifts provides a strong proxy to the overall informational data privacy climate. With that, consumers, and their behaviors relating to perception and trust, are a single actor within the actor-network system involving data and information privacy.

Within the United States, any idealization of a cohesive and thorough system of regulations to protect consumer's private data is unfounded (Klosowski, 2021). At the United States federal government level, data privacy regulation only targets certain types of information

or sectors, such as health and educational records. In the absence of federal guidance, only three states, including California, Colorado, and Virginia, have passed any form of data privacy legislation (Lively, 2022). Although not insignificant, the lack of federal guidance and low-level of state involvement in regulation leaves a piecewise solution to a tackle an issue that is truly one of national – or even global – scale. Within the actor-network, government institutions are an actor via their intervention, whether through existing or potential influence, in the market through regulatory responsibilities.

While each digital service or platform has its own set of guiding values and design decisions regarding how user data is handled, the underlying operating system developer retains significant control regarding system-wide constraints. In other words, a website or app that desires to collect or use personal data in a specific manner cannot do so on a device operating system that prohibits that exact method. Recently, users on Apple's iOS were provided a system feature to request apps not to track their data. When a user fails to opt-in for this tracking option on iOS, the operating system does not allow the app to access unique identifier codes traditionally used for tracking (Ha & Panzarino, 2021). Specifically, the choice was designed to be an opt-in consent system to allow tracking rather than the industry standard of an opt-out policy; this simple caveat is an example of user-centered design as the user's needs were ruled paramount to business desires (Vargas, 2021). Although this feature to request apps not to track does not preclude the app from collecting or using personal data in any capacity, it does restrict the ease and scope of what the app can feasibly accomplish. With conscious design decisions becoming commonplace regarding personal data privacy on operating systems, hardware and operating system developers are an influential actor in the actor-network.

With the major actors in the data privacy actor-network established, the linkages and networks between each of them can be revealed. As government regulation has potential to not only influence but also restrict the actions of all actors within the actor-network, it provides a logical starting point for analysis. Government interventions intended to safeguard personal data on the behalf of consumers are nearly nonexistent across the United States. However, in 2021, there was a renewed push in the United States Congress, with the introduction of five legislative bills, that both directly and indirectly, establish an unprecedented set of federal guidelines for data and information protection practices (Kang, 2021). Negotiations on this set of legislation is active throughout the duration of the 117th United States Congress that concludes in January of 2023 (Sykes, 2021). Notably, these bills are primarily targeted at so-called "big tech" firms, such as Facebook and Google, that hold extensive market capitalizations and power within the technology sector. Therefore, the proposed legislation is formulated from the viewpoint and legal standing of antitrust regulation (Kang, 2021). Although such regulation would be enacted with antitrust at its foundation, the impacts of such rules would not necessarily be limited to only those large firms as precedent for data privacy practices would be established. However, there would be little to no oversight or regulatory authority for small firms that did not adopt the newer standards from the established precedent. Therefore, while not insignificant, a federal solution regarding data privacy achieved through antitrust regulation would not provide robust, comprehensive guidelines to which all firms must adhere; this still results in gaps in protection for consumers.

To best understand how the current US approach to personal data privacy results in a shortfall, there is value in examining the approach taken by the European Union; their approach has taken nearly a direct reversal in ideology to the United States. The General Data Protection

Regulation, commonly referred to as the GDPR, is the EU's signature data privacy regulation that first went into effect in 2018. The GDPR relies upon the principle that both data privacy and data protection are fundamental human rights protected under doctrine (Barrett, 2019). GDPR is structured as a framework with multiple facets. The most discussed tenets include rights to be informed, of access, to rectification, and to erasure of one's private data (Burgess, 2020). These requirements aim to ensure that individuals understand what data firms collect and how it is used while maintaining ownership rights that allow for demanding erasure and some accountability on behalf of firm missteps. The foundational ideas to data privacy regulation in the European Union are almost entirely excluded from the current legislative narrative within the United States. Although the GDFR is not necessarily a final or perfect solution, it illustrates the gap between current regulatory approaches between the United States and other countries.

The right to data privacy and data protection does not exist in the United States under the Constitution. Therefore, a law similar to the GDPR in the European Union could not directly be applied in the United States. However, the driving ideas behind the regulation could be used as a starting basis for new legislation and regulation. If ideologically similar legislation came to fruition, the government would be able to empower consumers by shifting the balance of power away from the profit-seeking firms. Advancement of any such legislation would directly contrast the current regulations that leave nearly all power and control with the firms instead of the users or regulatory bodies. This empowerment of consumers would shift their perception of data privacy issues in a positive favor due to increased explicit information and ownership of their data.

Between the drive of for-profit firms to collect and use personal data and the US government's lack of any significant, adequate regulation to ensure consumer protection, the

trust users have on digital platforms is unstable. An empirical analysis regarding consumer trust of social media platforms identifies two influential factors that influence user trust: communication and opportunistic behavior (Kozánková & Kambule, 2021). When consumers perceive that firms offer high levels of transparency regarding data collection and use, they place higher levels of trust into the firm and its practices (Kozánková & Kambule, 2021). Within the concept of personal data, transparency is characterized by clear and succinct communication with the users on what policies are employed by the platform. Simply put, notifying users what data is collected, how it will potentially be used, and the guidelines that govern it forms an environment of trust.

Following a similar reasoning, increased consumer perception of firms engaging in opportunistic behavior is associated with lower levels of trust. Optimally demonstrated through a case study, opportunistic behavior is when a firm is viewed as taking advantage of one's personal data in search of desired monetary benefit (Kozánková & Kambule, 2021). This need not imply that all use of data is viewed by consumers as opportunistic; rather, such concept applies to events where the firm's action on an opportunity seemed either risky or unnecessary to the traditional or foundational functionality of the platform. For example, the collection of data on Facebook that was later utilized by third-party Cambridge Analytica in 2018 for political analysis was met with significant backlash and led to degraded trust in the company (Confessore, 2018). Consumers expect firms to operate within a reasonable realm of expectations. When firms fail to limit activities to such constraints, consumer trust suffers the consequences.

With the link established connecting firm privacy practices to consumer trust and perception, the next tranche to answer the subject of this research involves how aforementioned trust influences behavior. Consumer trust is directly correlated with data privacy transparency

and indirectly correlated with opportunistic behavior engagement; this results in translations on consumers by for-profit firm and technology developer actors within the network. However, understanding how such changes in trust influence consumer behavior is imperative to comprehending the impacts felt across the information and data privacy actor-network.

When consumers perceive less trust in a service or platform, they reduce their level of engagements and transactions with the respective technology. An empirical study conducted by Carlos Flavián and Miguel Guinalíu (2006), researchers of Business and Economics at the University of Zaragoza, concluded that "the development of trust not only affects the intention to buy… it also directly affects the effective purchasing behavior, in terms of preference, cost and frequency of visits, and therefore, the level of profitability provided by each consumer" (p. 12). The researchers not only established that decreasing consumer trust reduces consumer interaction or use of platforms but noted that trust is primarily built upon ideas of privacy and security. This finding, when incorporated with the other actors within the data privacy actor-network, indicates that there are broad ramifications for all actors when consumer trust fluctuates.

Primarily, when trust between users and platforms or services declines, the overall social benefit of their use decreases. Not only do for-profit firms potentially lose opportunities to generate revenue, and in-turn profits, but consumers are not able to capture the positive benefit of the service. For example, if a consumer does not trust an e-commerce clothing store and does not place an order due to such concerns, the business misses the potential for a sale to a new customer, and the consumer does not receive the good that they wished to purchase. As stated earlier, consumer behavior is not binary but rather takes a variable approach with the level of trust or concern. With that, an individual may limit their use of a platform to only when they deem the benefits outweigh the potential risk or downsides of using the service. In other words, a

user may use Facebook Messenger to contact family members abroad during a natural disaster but not for typical daily, check-in communications. While levels of trust are correlated with different activity levels, the direction of the relationship holds constant with less trust experiencing less interaction.

Equipped with an understanding of what factors influence consumer trust and how that trust alters their behaviors, business and government actors hold immense opportunity and power to shape digital technologies for the benefit of all parties. Employing a user-centered design approach during the development of technologies and data privacy regulations should aim to maximize consumer trust while weighing trade-offs on behalf of firms and enforcement burdens. As user-centered design approaches view the needs and desires of the consumer as the central focus of all objectives, consumer trust becomes built into designs rather than devised as an appended afterthought.

Profit-seeking firms can increase user interaction and customer loyalty by developing a culture of consumer trust. Although developing this trust may place restrictions on opportunistic behavior and necessitate increased transparency, the firm is rewarded with increased service use and potential revenue streams. For existing firms, the change to a business model structured around user information and data privacy trust may not be beneficial in the short-run, but it will yield positive surplus in the long-run. Additionally, as firms transition to a mindset that prioritizes consumer trust, those who fail to take such actions may be viewed as inferior and thus left behind in a competitive market economy. One significant implementation of such user-centered policies occurred in 2016 when Apple implemented a new technology known as differential privacy; this innovation enabled the collection of personal data for services dependent on user data while preserving user anonymity and confidentiality; this technology was

highly regarded by subject-matter experts (Conger & Lomas, 2016). Although business goals and user-centered design objectives do not always align in parallel, that does not indicate that technologies cannot be designed for the benefit of both parties.

Knowledge of how consumer trust is fostered and its associated impacts on behavior enable governments to draft effective and efficient legislation. All legislation should be both effective, meaning it accomplishes the intended objectives, and efficient, meaning the method used to reach the objectives minimizes disruptions and unnecessary burdens. Primarily, government regulation can be expanded to cover all actors within the actor-network and should prioritize requirements for information and data privacy transparency and detail a risk management methodology to firms who wish to pursue potentially opportunistic behavior. Implementing government regulation containing these ideas standardizes requirements across the sector leading to efficiency, clear protections for consumers, and the cultivation a digital technology environment built for the 21st century.

Research Study Limitations

The findings presented in this analysis answer the fundamental research question of how data privacy practices influence consumer trust and behavior. However, due to time and resource availability, the depth of the analysis was limited to a high-level scope. Mainly, there is limited existing literature that empirically links data privacy and consumer trust to a response in behavior. Although studies that view either the trust or behavior aspect in isolation still hold contextual value, it is difficult to develop accurate, concrete conclusions from them. Extending the significance of this limitation, the nature of this analysis did not enable for an active research study. Therefore, the literature used for background and supporting analysis was strictly constrained to preexisting information. Nevertheless, there was ample research available develop

a thoughtful analysis of data privacy as it relates to consumer trust and behavior through the sociotechnical lens of actor-network theory.

Recommendations for Future Research

With the idea established that information and data privacy practices do help shape consumer trust thus influence behavior, there are nearly endless routes for further research. Primarily, the findings of this study could be the foundation of research to understand the magnitude of trust and behavioral shifts stemming from privacy practices. A quantitative study into this topic would yield results that could help explain the optimal trade-off point to use for government regulations. Additionally, this research could be expanded to examine how the specific digital technology sector, such as healthcare, commerce, or social networking, influences the magnitude of consumer's behavioral response. While these ideas are not exhaustive of future research, they pose significant possibility for further advancing the field of data privacy and sociotechnical issues.

Conclusion

The primary actors of consumers, for-profit firms, developers, and governments are critical players within the information and data privacy actor-network. As the perception of information and data privacy practices influences customer behavior and trust, actors should take initiative to maintain consumer trust and behavior by way of user-centered design. The user-centered design should build upon foundational concepts of maximizing data practice transparency and mitigating risks of opportunistic behavior that are vital to affording positive consumer behavior. As society continues to progress further into the era of big data and the realm of artificial intelligence technologies, broadening the awareness and understanding of the

data privacy actor-network, through research such as this, provides tools for each actor to be proactive rather than reactionary to new technologies.

References

Anant, V., Donchak, L., Kaplan, J., & Soller, H. (2020). *The consumer-data opportunity and the privacy imperative.* McKinsey & Company. https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/he%20consumer%20data%20opportunity%20and%20the%20privacy%20imperative/The-consumer-data-opportunity-and-the-privacy-imperative.pdf

Auxier, B., Raine, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019). *Americans and privacy: Concerned, confused and feeling lack of control over their personal information*. Pew Research. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information

Balaban, D. C., & Mustățea, M. (2021). Privacy concerns in mobile communication. A user's perspective. *Philobiblon: Transylvanian Journal of Multidisciplinary Research in Humanities*, *26*(1), 101–114. https://doi.org/10.26424/philobib.2021.26.1.06

Barrett, L. (2019). *Confiding in con men: U.S. privacy Law, the GDPR, and information fiduciaries* (SSRN Scholarly Paper ID 3354129). Social Science Research Network. https://papers.ssrn.com/abstract=3354129

Bonner, W. (Bill). (2013). History and IS – Broadening our view and understanding: Actor–network theory as a methodology. *Journal of Information Technology, 28*(2), 111–123. https://doi.org/10.1057/jit.2013.6

Burgess, Matt. (2020). *What is GDPR? The summary guide to GDPR compliance in the UK*. WIRED. https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018

Cohen, M., Fahs, G., Moskowitz, B., & Nguyen, S. (2020). *Privacy front & center: Meeting the commercial opportunity to support consumers rights*. The Digital Standard. https://thedigitalstandard.org/downloads/CR_PrivacyFrontAndCenter_102020_vf.pdf

Confessore, Nicholas. (2018). Cambridge Analytica and Facebook: The scandal and the fallout so far. *New York Times*. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

Conger, Kate & Lomas, Natasha. (2016). *What Apple's differential privacy means for your data and the future of machine learning*. TechCrunch. https://techcrunch.com/2016/06/14/differential-privacy/

Cooke, L. (2018). Privacy, libraries and the era of big data. *IFLA Journal, 44*(3), 167–169. https://doi.org/10.1177/0340035218789601

Cressman, D. (2009). A brief overview of actor-network theory: Punctualization, heterogenous engineering & translation. https://summit.sfu.ca/item/13593

Flavián, C., & Guinalíu, M. (2006). Consumer trust, perceived security and privacy policy: Three basic elements of loyalty to a web site. *Industrial Management & Data Systems*, *106*(5), 601–620. https://doi.org/10.1108/02635570610666403

Floridi, L. (2005). The ontological interpretation of informational privacy. *Ethics and Information Technology*, *7*(4), 185–200. https://doi.org/10.1007/s10676-006-0001-7

Goddard, William. (2019). *How do big companies collect customer data?* IT Chronicles. https://itchronicles.com/big-data/how-do-big-companies-collect-customer-data/

Gothmann, Adam. (2021). *Data privacy day: How much do consumers really know about data privacy?* Security Boulevard. https://securityboulevard.com/2021/01/data-privacy-day-how-much-do-consumers-really-know-about-data-privacy/

Ha, Anthony & Panzarino, Matthew. (2021). *Apple's app tracking tracking transparency feature will be enabled by default and arrive in 'early spring' on iOS*. TechCrunch. https://techcrunch.com/2021/01/27/apple-app-tracking-transparency/

Kang, Cecilia. (2021). Lawmakers, taking aim at big tech, push sweeping overhaul of antitrust. *New York Times*. https://www.nytimes.com/2021/06/11/technology/big-tech-antitrust-bills.html

Klosowski, Thorin. (2021). The state of consumer data privacy laws in the US (and why it matters). *New York Times*. https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/

Kozánková, B., & Kambule, N. (2021). Consumer trust and data privacy: Precursors of trust towards social media in the age of data collection.

Kwet, Michael. (2019). In stores, secret Bluetooth surveillance tracks your every move. *New York Times*. https://www.nytimes.com/interactive/2019/06/14/opinion/bluetooth-wireless-tracking-privacy.html

Lively, Taylor. (2022). *US State privacy legislation tracker*. International Association of Privacy Professionals. https://iapp.org/resources/article/us-state-privacy-legislation-tracker/

Modell, S. (2020). For structure: A critical realist critique of the use of actor-network theory in critical accounting research. *Accounting, Auditing & Accountability Journal*, *33*(3), 621-640. http://dx.doi.org/10.1108/AAAJ-01-2019-3863

Obar, J. A., & Oeldorf-Hirsch, A. (2020). The biggest lie on the Internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, *23*(1), 128–147. https://doi.org/10.1080/1369118X.2018.1486870

Sykes, Jay. (2021). *The big antitrust bills*. Congressional Research Service. https://sgp.fas.org/crs/misc/R46875.pdf

United Nations. (2021). *The impact of digital technologies*. https://www.un.org/en/un75/impact-digital-technologies

Valkenburg, G., & van der Ploeg, I. (2015). Materialities between security and privacy: A constructivist account of airport security scanners. *Security Dialogue*, *46*(4), 326–344. https://doi.org/10.1177/0967010615577855

Vargas, Mariana. (2021). *How to balance user-centered design with business goals*. Medium. https://uxdesign.cc/how-to-balance-user-centered-design-with-business-goals-321c563222cc

Wang, Edward Shih-Tse. (2019). Role of privacy legislations and online business brand image in consumer perceptions of online privacy risk. *Journal of theoretical and applied electronic commerce research*, *14*(2), 59-69. https://dx.doi.org/10.4067/S0718-18762019000200106

World Economic Forum. (2012). *Big data, big impact: New possibilities for international development.* https://www3.weforum.org/docs/WEF_TC_MFS_BigDataBigImpact_Briefing_2012.pdf

Yaneva, A. (2009). Making the social hold: Towards an actor-network theory of design. *Design and Culture*, *1*(3), 273–288. https://doi.org/10.1080/17547075.2009.11643291

Your data is shared and sold…what's being done about it? Knowledge@Wharton (2019, October 28). https://knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done/