Balancing the Scale: Finding Common Ground on Internet Privacy

An STS Research Paper
presented to the faculty of the
School of Engineering and Applied Science
University of Virginia

by

Aaron Alem

March 15, 2024

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.

Aaron Alem

STS advisor: Peter Norton

Balancing the Scale: Finding Common Ground on Internet Privacy

About 62 percent of US adults accept daily data collection as a fact of life; 81 say they have no control over data collection (Auxier 2019). User data allows companies to offer free services and improve their products and services, however consumers do not alway feel these benefits are worth it. How can we find the optimal blend between digital privacy and digital utility? More often than not consumers are more weary now when it comes to giving up personal data. When data is used to make direct improvements to products/services, consumers believe that they are getting a fair trade. For example, when Netflix collects data to recommend shows or when Apple records user location to automatically keep track of where they parked their car, consumers feel that they are getting value despite reduced privacy. However, when big tech companies such as Meta Platforms, X Corp, or Google collect data for target marketing, consumers no longer see the value in this trade (Morey 2015). These concerns have been voiced by the public to government departments such as the Federal Trade Commission (FTC) who Chairman Joe Simons explains that, "is committed to protecting consumer data privacy," and "ensuring that social media companies (...) do not mislead individuals about the use of their personal information," (FTC 2019). Organizations like the Electronic Privacy Information Center (EPIC), a non-profit that maintains Americans' right to privacy have pushed for restrictions on the data broker industry and consumer protections. This has led to the implementation of new laws that help increase online privacy. In 2023 alone, 14 US states have implemented consumer data privacy laws that limit the types of data that can be collected and allow users to opt out of personal data collection. Advertising companies have also seen the outcry for more consumer protections on personal data and have come together to create the Digital Advertising Alliance (DAA). Through the DAA, advertising companies attempted to self-regulate online advertising

and “Provide standards and transparency for digital advertising,” (Signorelli 2018). However, with 81% of Americans believing that the potential risks of collecting data on them outweigh the benefits (Auxier 2019), there’s still a big disconnect between companies and consumers on digital privacy. In order to bridge this gap, companies must prioritize building trust with consumers.

Scholarly Exploration

Hallam and Zanella (2016) observed that despite most expressing concerns for privacy, people constantly share sensitive information online using social networking sites. This creates something they call a “privacy paradox”. This “privacy paradox” is demonstrated in social networking sites where privacy risks are seen as abstract while social rewards are seen as concrete. Construction level theory tells us that ideas considered abstract are associated with distant-future outcomes while concrete ideas are associated with near-future ones. Since distant-future outcomes tend to be discounted for near-future ones, online privacy is discounted for social rewards. Consumers are willing to sacrifice their privacy for believed benefits. In this scenario, social rewards are seen as worthy compensation. Liu and Pavlou (2021) looked to improve privacy policies for consumers using information technology. They prototyped an “active-recommendation” feature which uses customer service agents to allow consumers to customize their own privacy policies. To test its effectiveness, Liu and Pavlou made three apps, each with a different way of displaying the privacy statement and compared the acceptance rates. App 1 had a link to the statement and had users select “agree" or “disagree”. App 2 allowed consumers to select their privacy settings before agreeing or disagreeing. App 3 implemented the “active-recommendation” feature. App 1 had the highest acceptance rate, but only a percentage of users read the privacy policy. App 3 gave users the best experience by reducing their cognitive

load and allowing them to understand the level of privacy they were giving up. Consumers are more willing to give up privacy when they can understand the tradeoffs. Nget, Cao, and Yoshikawa (2018) set out to find a balance between money and protection of personal data through a data market. After taking a survey to estimate the type and value of information that will be sold, pricing for different types of data were made. Using this pricing, they were able to create a framework for a personal data market that more fairly compensates people for the loss of their privacy. Wang, Wang, and Zhang (2021) explored digital privacy from different perspectives and narrowed it down to three main ideas. These ideas are privacy as a technical artifact, psychological need, and economic tradeoff. When looking at privacy as a technical artifact, a solution was found where using machine learning models sent masked results which ensured privacy of the user. In the psychological need for privacy, a new construct, "peer privacy concern," was found. This idea was that people feel that it is impossible to maintain their privacy due their peers being online. When exploring privacy as an economic tradeoff Chong Wang, Cong Wang, and, Zhang found the same "privacy paradox" as mentioned earlier.

Digital Privacy: The Necessity of Transparency

Transparency is an important part of digital privacy. If companies want to build trust with consumers, they need to be transparent on when and what the data is being collected. Advertising companies have begun to see the importance of transparency with users, with some implementing policies and features to help improve it. In June 2023 the Digital Advertising Alliance released a document named "DAA Best Practices." Lou Mastria, CEO of the DAA states that this, "Will kick off a creative ad specification process, so we can help consumers access privacy information and controls for connected devices through intuitive notices and

consolidated user interfaces." This will guide companies towards collecting data from connected devices such as smart appliances, TV's, smartwatches, etc. in a way that is transparent with the consumer. When collecting data from these kinds of devices, disclaimers that data is being collected will be shown in addition to an option for users to limit the collection of data. The "DAA Best Practices" also looks towards making sure consumers know about data being collected from companies outside the DAA. Lou Mastria sees how important it is to be transparent about the data being collected. Specifically, he says "The DAA has issued these best practices to drive forward the adoption of enhanced transparency and control for companies creating connected products and services." When consumers know their data is being collected and have the option to stop it, they can more easily trust companies. This trust then makes consumers more comfortable with giving away data they normally would not. Companies outside of the Digital Advertising Alliance are also seeing the importance of transparency in data collection. Apple has multiple resources that allow consumers to learn more about how their data is being used and how to protect it. In all Apple stores, Apple has offered free courses that teach users how to use privacy features on their devices. They have also released videos that give examples of how data collection is often abused. In addition to these resources, Apple has released features that give users an understanding and control of how their data is being used. Apple now requires all apps to "give users an easy-to-view summary of the developer's privacy practices," (Apple 2021). Apple has also implemented "App Tracking Transparency" which will "require apps to get the user's permission before tracking their data across apps or websites owned by other companies," (Apple 2021). Apple is very committed towards giving its users transparency and control of their data. Erik Neuenschwander, director of User Privacy at Apple also shares this sentiment as he states "Over the years we've integrated powerful privacy controls

into our operating systems. This film and our new Today at Apple sessions will show users how they can take advantage of some of the features we offer, and understand how privacy is at the center of everything we do," (Apple 2023). This commitment towards giving users transparency has led towards an increase in trust between consumers and Apple, with people publicly praising the work they have done. Privacy International is a non profit that works to protect the human right of privacy across the globe (PrivacyInternational n.d.). Gus Hosei, an executive director at Privacy International said, "Where there is a lack of transparency, exploitation thrives. Invisible and gratuitous data collection leaves users unable to exercise their rights and protect their privacy. Apple's nutrition labels require industry to be clear and upfront with consumers, and tools like App Tracking Transparency will help people to assert control over the invisible leakage of their data. With these commendable innovations, industry will finally feel pressure to change." Additionally, Tristan Harris, cofounder of Center for Humane Technology which is a non profit that works to"align technology with humanity's best interests," (Center For Humane Technology, n.d.) has also praised Apple's efforts. Tristan Harris states, "Today's Apple announcement moves the ecosystem further away from the malicious effects of secretive profiling and microtargeting," and "Awareness of industry practices like data tracking is only the first step toward a better privacy experience," (Apple 2021). Both Harris and Hosei show that allowing for more transparency in data collection allows for more trust and a better privacy experience for the consumer as they no longer feel they are being exploited.

Digital Privacy: Accountability and Regulation

Companies have already made it hard for consumers to trust them as repeatedly they have gone against their word. After the Supreme Court rescinded the constitutional right to abortion in 2022, Google stated that if "its systems identified that a user had visited an abortion clinic, it would delete these entries from Location History soon after they visit," (EPIC 2024) in order to promote trust from its users. However, months later it was proven that Google actually had not deleted this location information that they said they would. Soon after Google had again promised to "extend enhanced protections to users' location data," but a year later they have still not made any changes. The Electronic Privacy Information Center has expressed how harmful the outcomes of Google not following through on their promise can be in a complaint they filed against Google to the FTC. Specifically, they state, "Google's personal location data practices have caused or are likely to cause substantial injury to its users because they expose users to excessive retention of their 'particularly personal' information that can reveal highly sensitive information about them, including whether an individual visited a medical treatment facility, domestic violence shelter, abortion clinic, fertility center, addiction treatment facility, or a surgery clinic," and "The ability of law enforcement to access such data can lead to criminal prosecution and unduly discourage individuals from seeking vital health care services—a risk of substantial injury that has dramatically increased following the Dobbs ruling," (EPIC 2024). This lack of care from Google has put its users at risk which has destroyed the trust between Google and its users. This has made it far harder for users to further trust Google in the future in regards to data collection. EPIC Counsel Sara Geoghegan further explains that, "These harmful practices show us why we cannot rely on pinky promises from Google to protect our most sensitive information," (EPIC 2024). This opinion is further expressed by Kaili Lambe, Policy and

Advocacy Director at Accountable Tech. Accountable Tech is a non profit that works “to curb the societal harms driven by Big Tech’s toxic business practices,” (AccountabeTech 2024). Kaili Lambe states that, “Google can’t have it both ways. If the company wants the reputation of being strong on privacy protection, it must live up to its commitments – not merely pay them lip service. But over and over again Google has broken its promises, risking the personal data of the people who rely on its services. Google can’t be trusted, which is why we’re asking the FTC to investigate.” The US Government has also failed in assuring people that their data is not being exploited. On February 1, 2024, EPIC released a report named, “ The State of Privacy: How State ‘Privacy’ Laws Fail to Protect Privacy and What They Can Do Better.” In this report, EPIC investigated and graded each of the states that passed online privacy laws on their ability to protect consumers. From this investigation, it was found that “nearly half of the 14 states that have passed so-called comprehensive privacy laws received a failing grade, and none received an A,” (EPIC 2024). Caitriona Fitzgerald, deputy director of EPIC, expressed her frustrations with these poor laws. She states, “Many of these ‘privacy laws’ protect privacy in name only. In effect, they allow companies to continue hoarding our personal data and using it for whatever purposes they want.” Because of these broken promises from companies and lack of protection from the government, consumers feel that neither companies nor the government are working to protect their online privacy. This has led to consumers distrusting companies when it comes to data collection. If companies want to find a balance between allowable and non-allowable data collection, they need to rebuild this trust.

Digital Privacy: True Value of Data

Consumers find it easier to give up data when they understand the reason behind the collection of their data. Companies like Meta (Formerly "Facebook") strive towards growing their business and increasing their number of users of their services. To do so, they created social media platforms they believe are "inherently personalized," through providing tailored ads. They believe that these ads are "a necessary and essential part of the service," (Bushard 2023). To create this personalization, Meta collects large amounts of personal data. The benefits of this data collection was not obvious and users were weary about the data being collected. While Meta did, "promise users they can control the privacy of their information through Facebook's privacy settings," (FTC 2019) users still felt that their privacy was being abused. This distrust led to the FTC overhauling the way the company makes privacy decisions by, "boosting the transparency of decision making and holding Facebook accountable via overlapping channels of compliance." Meta was forced to create an independent committee for decisions involving privacy and submit quarterly certifications that the company is in compliance with the FTC's privacy program. The International Association of Privacy Professionals (IAAP) is an organization that strives "to define, promote and improve the privacy profession globally," (IAAP n.d.). In 2023, they released the "Privacy and Consumer Trust - Executive Summary" which provides information on "how individuals value their privacy and the steps they will take to protect it," (Fazlioglu, 2023). In it it states that "Few consumers said it is easy for them to understand whether a company follows good privacy practices. The majority of consumers had limited understanding of the types of personal data collected about them." Consumers are clearly confused on what data is collected and used for. This has led them to lose trust in companies like Meta as when data is only being used for target advertising, consumers do not feel that their data should be collected

for this reason. Organizations such as the American Civil Liberties Union (ACLU) have spoken out against data collection for this reason. The ACLU is a non profit organization that works towards protecting the individual rights of Americans changing policy. ACLU Executive Director Ira Glasser believes that privacy is an important thing to protect. Specifically he states, "The Fourth Amendment still protects the privacy of our homes, but personal information isn't exclusively stored there anymore. Now, a wide array of personal information about each of us is kept electronically by others — by medical insurers, employers, credit card companies, banks, phone companies and a wide range of government and private agencies." Glasser is against data collection for targeted advertising as he believes, "these entities exist solely to sell our personal information, no matter how private. And new technologies keep arising to develop, collect, store and disseminate the most private information about each of us, with few if any legal protections." To help fight against this "theft" of personal technology, the ACLU released a website with multiple different features that give individuals the ability to help personally protect their individual online privacy. Target advertising and data collection in general that does not benefit users is usually disliked by consumers. If Companies give users observable value for their data that consumers believe is fair, they are more likely to be trusted. Through this trust, consumers and companies will be able to come to an agreement on the allowable data collection.

Conclusion

Trust is a crucial factor in companies and consumers alike finding a balance between what type of data collection should be allowed. To create this trust though, there are a multitude of things companies must do. When collecting data, companies must be fully transparent in when data is being collected and what kind of data is being collected. In addition to this, it must be

shown in a format that is easy to find and understand. This will allow for consumers to feel more comfortable as they know exactly what is going on and no longer have to feel that they are being exploited. Companies also must work towards regaining consumers' trust by following through on expectations. As consumers' trust has already been fractured by past experiences, these companies must work hard to bring back the trust so consumers will be more willing to share their data. The government must also play a part in recreating this trust. With better privacy laws, consumers will feel protected by the government from exploitation. With these protections, there will be less fear in consumers and they will be more willing to give up their data. Lastly, companies need to use data to make visual improvements to their products. Data holds value to the user, and in giving up that data, users expect something in return. When data is collected exclusively to be sold to advertisers, users do not see any value gained from the loss of their privacy. If companies want consumers to give up their reduced privacy, they must give them something in return.

References

Accountable Tech. (n.d.). *About*. https://accountabletech.org/about/?cn-reloaded=1

ACLU. (2019). *About the ACLU. American Civil Liberties Union.* https://www.aclu.org/about-aclu

American Civil Liberties Union. (1999, March 8.). *ACLU Launches Special Web Collection On Privacy and Data Protection.* https://www.aclu.org/press-releases/aclu-launches-special-web-collection-privacy-and-data-protection

Apple Newsroom. (2023, January 24). *Apple builds on privacy commitment by unveiling new efforts on Data Privacy Day.* https://www.apple.com/newsroom/2023/01/apple-builds-on-privacy-commitment-by-unveiling-new-efforts-on-data-privacy-day/

Apple Newsroom. (2021, January 27). *Data Privacy Day at Apple: Improving transparency and empowering users* https://www.apple.com/newsroom/2021/01/data-privacy-day-at-apple-improving-transparency-and-empowering-users/

Auxier, B. (2019, November 15). *Americans and privacy: Concerned, confused and feeling lack of control over their personal information.* Pew Research Center: Internet, Science & Tech. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Bushard, B. (2023, January 4). *Meta Fined Over $400 Million By EU For Alleged Personal Data Collection Violation*. Forbes. https://www.forbes.com/sites/brianbushard/2023/01/04/meta-fined-over-400-million-by-eu-for-alleged-personal-data-collection-violation/?sh=459bdfff5592

Center for Humane Technology. (n.d.). *Who We Are.* https://www.humanetech.com/who-we-are

Digital Advertising Alliance. (2023, June 15). *Digital Advertising Alliance Releases Best Practices Around Privacy for Billions of IoT Connected Devices.* https://digitaladvertisingalliance.org/press-release/digital-advertising-alliance-releases-best-practices-around-privacy-billions-iot

Digital Advertising Alliance. (n.d.). *Integrate with DAA's CCPA Opt-Out Tool.* https://digitaladvertisingalliance.org/integrate-webchoices-ccpa

Electronic Privacy Information Center. (2024, January 18). *PRESS RELEASE: EPIC, Accountable Tech Urge FTC to Investigate Google's Failed Promise to Delete Sensitive Location Data*. https://epic.org/press-release-epic-accountable-tech-urge-ftc-to-investigate-googles-failed-promise-to-delete-sensitive-location-data/

Electronic Privacy Information Center. (2023, January 16). *PRESS RELEASE: EPIC Announces Organizational Updates for 2023*. https://epic.org/press-release-epic-announces-organizational-updates-for-2023/

Electronic Privacy Information Center. (2023, July 17). *PRESS RELEASE: EPIC Urges CFPB to Take Decisive Regulatory Action Against Data Brokers.* https://epic.org/epic-urges-cfpb-to-take-decisive-regulatory-action-against-data-brokers/

Electronic Privacy Information Center. (February 1, 2024). *RELEASE: Report: State Laws are Failing to Protect Privacy.* https://epic.org/release-report-state-laws-are-failing-to-protect-privacy/

Federal Trade Commission. (2022, January 27). *FTC imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook.* https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook

Ford, N. (2023, October 6). *List of data breaches and cyber attacks in 2023*. IT Governance UK Blog. https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023#:~:text=According%20to%20our%20research%2C%20there,total%20to%20over%204.5%20billion

Fazlioglu, M. (2023, March). *IAPP Privacy and Consumer Trust Report – Executive Summary*. https://iapp.org/resources/article/privacy-and-consumer-trust-summary/

IAPP (n.d.). *Mission and Background.* https://iapp.org/about/mission-and-background/

Morey, T., Forbath, T., & Schoop, A. (n.d.). *Customer data: Designing for Transparency and Trust*. Harvard Business Review. https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust

Privacy International. (n.d.). About Us. https://privacyinternational.org/about

Signorelli, F. A. (2018, May 23). *Campaigns & Elections quotes Michael Signorelli in an article about the digital advertising industry's transparency initiatives*. Venable LLP. https://www.venable.com/about/news/2018/05/campaign-election-mike-signorelli-ad-indust-transp