The Struggle for Digital Privacy in the United States

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

by

Jackson Quinn

May 9, 2023

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.

Jackson Quinn

STS Advisor: Peter Norton

How are social groups in the United States fighting to protect digital privacy?

Companies collect vast user data online. For example, online accounts typically require users to enter personal information; apps often track user location. Users seldom know exactly what data is being collected. According to Golbeck and Mauriello (2016), “fewer than 60% of app users were aware that apps could access particular data points.” Nevertheless, many Americans say they value personal data privacy. In a study, Simko et al. (2022) found that “approximately 63%” of respondents “said they would be somewhat or extremely likely to download a contact tracing app with perfect privacy, while many fewer would download an app that shared their location with their government.” A 2015 Pew Research study found that “93% of adults say that being in control of who can get information about them is important” (Madden & Rainie, 2015). Throughout the United States, privacy advocates are fighting for better digital privacy protections. Data collectors invoke values such as free enterprise, user responsibility, and user convenience. To fight back, privacy activists appeal to principles such as individual rights, civil liberties, personal autonomy, and basic fairness.

Review of Research

In 1999, Intel’s new Pentium III processor was faulted for compromising user privacy; critics publicized their objections online (Leizerov, 2000). Such advocacy techniques have since proliferated. During the coronavirus pandemic, Msughter (2020) noted a similar phenomenon: “The proliferation of the information and communication technologies gadgets has contributed to the active participation of citizens in the creation and dissemination of media content, hence the emergence of what is globally recognized as citizen journalism” (Msughter, 2020).

The study of privacy among different age groups in society is common. Tao and Shuijing (2020) did a case study on elderly people in China, and found that elderly people were much more likely to be less aware about privacy protection online and were more likely to be forthcoming with information. Blank, Bolsover, and Dubois (2014) found that young people, as well as those who are more educated, are more likely to check their privacy settings.

Several papers have covered ways to measure levels of digital privacy. One such method is the Digital Privacy Divide (DPD) Index (Alhazmi, Imran, & Abu Alsheikh, 2022) . This index explores the socio-demographic inequalities in digital privacy. Balebako et al. (2012) developed a tool to measure how effective various tools were at limiting behavioral targeting in advertisements. Eckhoff & Wagner summarize over 80 privacy metrics that can be used to measure various traits such as anonymity, privacy, linkability, etc. (Eckhoff & Wagner, 2018).

The Data Collectors

Large internet-based businesses such as Google collect a wide range of user data. In 2018, Google claimed to have 1.5 billion users (Gmail, 2018). Google, in its terms, states that it uses the data to “deliver our services, maintain and improve them, develop new services, measure the effectiveness of advertising, protect against fraud and abuse, and personalize content and ads you see on Google and on our partners’ sites and apps” (Google, n.d.-a). Google tells its customers that its data collection practices improve the user experience. However, this is not always the case. According to Dukes, Hendrickson, & Burns (2018), in 2017, “Raleigh police used search warrants to demand Google accounts not of specific suspects, but from any mobile devices that veered too close to the scene of a crime.” Google permits users to control which of their data are collected. Google highlights such user controls: “You can control what information is used to personalize ads and manage your ads preferences with My Ad Center" (Google, n.d.-b). Google does address concerns of sharing data with government entities in their Requests for User Information FAQs page: "Google carefully reviews each request to make sure it satisfies applicable laws. If a request asks for too much information, we try to narrow it, and in some cases we object to producing any information at all" (Google, n.d.-c). There are options in the Google account settings to change location history saving, personalized ads and search results, and who can see the information displayed on your profile (Google, n.d.-d). Such preference settings, however, are not consistently reliable. Researchers have found that Google still stores location data even when the user had turned "Location History" off (Nakashima, 2018). Data collectors are often secretive, and cannot always secure user data. Another concern in the modern age of technology is data breaches. One of the largest known data breaches was that of Yahoo in 2016 (White, 2021). An estimated 500 million users were affected by this breach, and the breachers obtained data such as email addresses, phone numbers, dates of birth, hashed passwords, and answers to security questions. Where your data ends up is not always up to the companies that collect your data.

In 2009, as a response to concerns from Facebook users about the update to their terms of service, Facebook posted a blog detailing their views on the digital privacy of their users (Facebook, 2009). Michael Zimmer pointed out that this blog post often replaces the word 'privacy' with the word 'control', implying that it is up to the user to control what happens to their data (Zimmer, 2014). "This rhetorical maneuver helps minimize the responsibility of corporations to improve default levels of consumer privacy" (Draper, 2016). This is related to the concept of choice architecture. There are ways to frame choices in order to make certain outcomes more likely than others. For example, making certain settings the default when you create a Facebook account could make it more likely that the user would keep these settings. If Facebook did care about you being in control of your data, would it not make sense to make conservative privacy settings the default? This would allow users to make changes, but would not immediately share their user data with anyone. Whether through negligence or not, Facebook creates privacy choices for their users in a manner that doesn't promote digital privacy. Pedro Hartung through the United Nations Children's Fund (UNICEF) points out that "the idea that digital citizenship is achieved within the family or through classroom education on media literacy is an argument frequently used by tech companies" (Hartung, 2020). Hartung points to an infographic created by Google, in which they argue for better online safety education within schools (Google, n.d.-e). Again, we see a company shifting responsibility to another entity, this time the public education system. This is especially concerning with the rise of internet usage by children. It has been shown that many children do not fully understand how their data is being collected and what it is used for (Sun et al., 2021).

Snapchat added an AI chat feature in April of 2023 called My AI (Snapchat, 2023). Many users noticed inconsistencies in whether the AI had access to the user's location or not. One twitter user, @akidfromhafia posted a screenshot and screen recording of his chat with My AI. In the screen recording My AI turns his location off after @akidfromhafia requests the AI to do so. Then @akidfromhafia asked My AI for the closest gas station, and the AI was able to provide him with that information despite saying "I can't see your location anymore" (@akidfromhafia, 2023). Many other users on Twitter saw a similar phenomena in their chats with My AI. This shows that AI technology being implemented by companies has the ability to see your data and lie to the user about what data they can see.

Civil Liberties Advocacies

The American Civil Liberties Union (ACLU) protects digital privacy rights (*United States v. Carpenter et al,* 2015). Like the ACLU, the Electronic Privacy Information Center (EPIC) also litigates to protect digital privacy, including in the workplace (*United States v. Hamilton,* 2012). This is the first paragraph on ACLU's Internet Privacy page: "The ACLU works in courts, legislatures, and communities to defend and preserve the individual rights and liberties that the Constitution and the laws of the United States guarantee everyone in this country." (ACLU, n.d.). Their language appeals to those who have faith in the constitution, and convey the belief that your rights are in fact currently being violated. Digital privacy standards can impede law enforcement. EPIC takes a different stance. They convey the message that laws and codes regarding digital privacy in America need to be improved. This indicates their belief that your digital privacy is not necessarily being violated under current U.S. law. Their Data Protection page reads: "Organizations that choose to collect and use personal data take on obligations for the collection, storage, and use of the data. These obligations help ensure fairness, accountability, and transparency in decisions about individuals. Data Protection laws should build on the U.S. Code of Fair Information Practices and OECD Privacy Guidelines, which are widely followed and form the basis of other data protection regimes" (EPIC, n.d.). The Electronic Frontier Foundation (EFF) also promotes digital privacy, in part through publicity. An EFF press release, for example, embeds a warning in its headline: "Data Broker Helps Police See Everywhere You've Been with the Click of a Mouse: EFF Investigation" (EFF, 2022). EFF shares a similar view to EPIC, with their Privacy page stating: "National and international laws have yet to catch up with the evolving need for privacy that comes with new digital technologies" (EFF, n.d.). Like ACLU and EPIC, EFF also files lawsuits.

Digital Privacy Oriented Products and Systems

While it is concerning that law enforcement and other legal entities may be handling your digital data, there are tools created to make the handling of your data more secure. One product offered by Veritone, Veritone Redact, is "developed for law enforcement, judicial agencies and legal & compliance teams" (Veritone, 2022). This product offers tools such as blurring of faces in videos and redaction of personally identifying audio. While this is not a solution to prevent your data from being used by law enforcement agencies, it can help prevent that information from leaking out into the public. With a virtual private network (VPN), users can access locally restricted web pages or to mask their location. ExpressVPN, a popular VPN in the U.S., advertises "If privacy is important to you, you should use a VPN every time you connect to the internet" (2023). To protect privacy, the Tor Project (Tor), a nonprofit, developed an onion routing network that anonymizes internet browsing. According to the Tor Project (2021), its mission "is to advance human rights and freedoms by creating and deploying free and open source anonymity and privacy technologies, supporting their unrestricted availability and use, and furthering their scientific and popular understanding." If you want to use your normal Internet browser, DuckDuckGo provides a search engine you can use within your browser. "Our privacy policy is simple: we don't collect or share any of your personal information" (DuckDuckGo, n.d.).

In "cybervetting," prospective employers now use personal data to screen job candidates. Users of social media in the U.S. are less likely to approve of cybervetting techniques than their counterparts in India; the difference may perhaps be attributable to culture or to differences in employment opportunities (Gruzd, Jacobson, & Dubois, 2020). One of the concerns with cybervetting is that it treats humans as if they had one identity. It ignores the fact that humans communicate differently to different people. When speaking more casually to friends you might speak in ways that are not acceptable by professional norms. An article by José van Dijck says "The mantra of people having one authentic or 'true' identity not only bespeaks a conspicuous ideology, playing into the hands of agencies and governments who want to control individuals' conduct, but also betrays a fundamental misjudgment of people's everyday behavior" (van Dijck, 2013). Nostr, which stands for Notes and Other Stuff Transmitted by Relays, is a social media and bitcoin exchange platform that is used by many as a replacement for Twitter. Many users use the Nostr platform to post anonymously and without fear of censorship. An anonymous Reddit user, u/cryotosensei said in 2023 he loves Nostr "Because you are only known by your public key, your privacy is secured as you don't doxx yourself by having to offer personal information about yourself."

Users also have the ability to improve the security of their data. One way is to improve the strength of the passwords they use, to make it more difficult for hackers to access their accounts. LastPass is a company that lets you create and store strong passwords. "You remember your vault password. LastPass remembers the rest" (LastPass, n.d.). Their service also includes monitoring of data breaches and alerts if your account information is found in databases on the internet and the "dark web".

Digital Privacy Conscious People

While the organizations discussed above do exist to promote digital privacy, there are other, less organized groups made up of privacy conscious individuals who also promote digital privacy. A couple of these groups can be found on the social media platform Reddit. For those who don't use Reddit, Reddit is divided into groups called 'subreddits'. These subreddits are focused on particular topics, and Reddit users are able to join them and see posts and commentary from other “Redditors" relating to that particular topic. These subreddits are denoted as ‘r/InsertSubredditNameHere’. For example, one of the most popular subreddits is r/gaming, which is dedicated to sharing and talking about anything related to gaming (video games, board games, etc.). For digital privacy, there are a couple of subreddits. The first is r/privacy with almost 1.3 million members (r/privacy, n.d.) and the second is r/privacyguides with 53.5 thousand members (r/privacyguides, n.d.). These subreddits are similar in the type of content that their users share. Things like news articles, personal privacy anecdotes, and privacy tips are frequently shared for the community members to see. While not conventional, a community working to keep one another informed on the current state of digital privacy can be effective in creating a more privacy conscious population. It is also a great way for users to stay up to date with current information regarding their digital privacy.

Movements in the form of protests have also been ways in which privacy conscious citizens fight to protect their digital privacy. Stop Watching Us was a protest that took place on October 26, 2013 in Washington D.C. (Newell, 2013). This protest along with The Day We Fight Back, an online protest on February 11, 2014, followed the widely publicized Edward Snowden leaks. The online The Day We Fight Back protests featured a website that included banners and other materials that people could display on their own websites across the internet (TheDayWeFightBack.org, 2014). They used multiple techniques to rally protestors and others around this cause. Till Wäscher looked at the movements through the lens of action frames, which they defined as “action-oriented sets of beliefs and meanings that inspire and legitimize the activities and campaigns of a social movement organization” (Wäscher, 2016). They listed four groups of action frames including “History of Surveillance,” “Orwellian Totalitarianism,” “Global Dimension,” and “Celebrity Activism.” Both History of Surveillance and Celebrity Activism can be seen in a video by Euronews where a protester holds a sign at the 11 second mark reading “We the People oppose the surveillance state and say thank you Edward Snowden” with a picture of Edward Snowden’s face (Euronews, 2013). In the same video, at the 18 second mark you can see the sign of another protestor reading “1984 was a work of fiction not an instruction manual”, showcasing the use of Orwellian Totalitarianism as a means to compare the current state of US surveillance to the popular novel *1984* written by George Orwell. In a video posted to Youtube by EFForg, the use of Celebrity Activism is seen throughout the video as multiple celebrities are seen talking about the collection of American citizens’ data by the NSA (EFFnews, 2013).

In 2014, Edward Snowden appeared on the TED Talk “Here’s how we take back the Internet”. At the 8:50 mark he gave a recommendation to web-based companies, “All companies need to move to an encrypted browsing habit by default for all users who haven’t taken any action or picked any special methods on their own” (Snowden, 2014). Later in the talk, at 13:09, while discussing why people should care about the American government collecting data from their citizens he said, “Beyond that, it’s a part of our cultural identity, not just in America, but in Western societies and in democratic societies around the world” (Snowden, 2014). Similar to ACLU, he chose to invoke traditional American values to gather support for the cause.

Generalizing the Strategies

The fight to protect digital privacy spans a wide range of methods. Data collectors shift the language they use to make the consumer feel more at ease. Data collectors also design choices to ensure the collection of more consumer data. To fight this, civil liberty advocates use legal channels to affect policy surrounding digital privacy. They preach to consumers that it is their right to have digital privacy, often invoking constitutional values. Companies create products to solve various digital privacy issues, and market them as necessary tools to protect your data online. Finally, digital privacy conscious people create online communities through which knowledge can be freely shared. These privacy conscious people create movements both in person and online and invoke traditional American values to voice their privacy concerns. For in person movements they use symbols to portray ‘American heroes’, use familiar celebrity faces as voices, and suggest a state of ‘Orwellian Totalitarianism’ to bring support to their cause. The online protests made it easier for anyone to get involved, helping to solve the free-rider problem, as posting a simple graphic takes much less commitment than attending a protest in person.

Conclusion

Data collectors regularly shift the language surrounding your privacy, sometimes appearing to be unintentional or beneficial to the consumer. Generally, it is important to use precise language. Those who seek control rely on you to concede the use of certain language in hopes that it may change the way you think. Fighting in the courts is important to create long lasting change, but spreading awareness is vital in the short term. Creating online communities to spread awareness and organize protests, especially those that are online, allow mildly concerned citizens to engage, when they otherwise wouldn’t. Future research could look at the methods discussed above and other methods of fighting for digital privacy and evaluate their effectiveness.

References

@akidfromhafia. (2023, April 24). Experimented chatting with snap AI… (Twitter). twitter.com/akidfromhafia/status/1650357441048002560

ACLU. (n.d.). Internet Privacy. aclu.org/issues/privacy-technology/internet-privacy

Alhazmi, H., Imran, A., and Abu Alsheikh, M. (2022). How do socio-demographic patterns define digital privacy divide? *IEEE Access*, *10*, 11296–11307. doi.org/10.1109/access.2022.3144436

Balebako, Cranor, Leon, Shay, Ur, and Wang. (2012). Measuring the Effectiveness of Privacy Tools for Limiting Behavioral Advertising. richshay.com. richshay.com/pubs/EffectivenessBA.pdf

Blank, G., Bolsover, G., and Dubois, E. (2014). A new privacy paradox: Young People and Privacy on social network sites. *SSRN Electronic Journal*. doi.org/10.2139/ssrn.2479938

Draper, N. A. (2016, Nov. 26). From privacy pragmatist to privacy resigned: Challenging narratives of rational choice in Digital Privacy Debates. *Policy & Internet*, *9*(2), 232–251. doi.org/10.1002/poi3.142

DuckDuckGo. (n.d.). Tired of being tracked online? We can help. duckduckgo.com/?va=b&t=hc

Dukes, T., Hendrickson, D., & Burns, M. (2018, March 13). To find suspects, police quietly turn to google. WRAL.com. wral.com/Raleigh-police-search-google-location-history/17377435/

Eckhoff, D., and Wagner, I. (2018). Technical Privacy Metrics: A Systematic Survey. *ACM Comput. Surv. 51(3)*. doi.org/10.1145/3168389

EFF (2022, Sep. 1). Electronic Frontier Foundation. Data broker helps police see everywhere you've been with the click of a mouse: EFF investigation. eff.org/press/releases/data-broker-helps-police-see-everywhere-youve-been-click-mouse-eff-investigation

EFF (n.d.). Privacy. eff.org/issues/privacy

EFFnews. (2013, Oct. 23). Stop Watching Us: The Video. (Youtube Video). youtube.com/watch?v=aGmiw_rrNxk

EPIC. (n.d.). Data Protection. epic.org/issues/data-protection/

Euronews. (2013, Oct. 27). 'Stop Watching Us' anti-mass surveillance rally in Washington. (Youtube Video). 0:11-0:20. youtube.com/watch?v=R3gRm0mHkII

ExpressVPN. (2023). What is a VPN? Expressvpn.com

Facebook. (2009, Feb 16). On Facebook, People Own and Control Their Information. (Blog post to Facebook.com). facebook.com/notes/10160195093241729/

Gmail. (2018, Oct 26). 1.5 billion users … (Twitter) twitter.com/gmail/status/1055806807174725633?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1055806807174725633%7Ctwgr%5Ecfc27a517ef40b8aa62a9d8b4cb4dd3fbb4d5364%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.androidpolice.com%2F2018%2F10%2F26%2Fgmail-now-1-5-billion-active-users%2F

Golbeck, J., and Mauriello, M. L. (2016). User perception of Facebook app data access: A comparison of methods and privacy concerns. *Future Internet*, *8*(2), doi.org/10.3390/fi8020009

Google. (n.d.-a). Privacy and Terms. policies.google.com/technologies/partner-sites?hl=en-US

Google. (n.d.-b). Safety Center. safety.google/privacy/ads-and-data/

Google. (n.d.-c). Requests for User Information FAQs. support.google.com/transparencyreport/answer/9713961?hl=en#zippy=

Google (n.d.-d). Data & Privacy. myaccount.google.com/data-and-privacy

Google. (n.d.-e). Digital Responsibility. *Google for Education*. edu.google.com/future-of-the-classroom/digital-responsibility/?modal_active=none

Gruzd, A., Jacobson, J., and Dubois, E. (2020). Cybervetting and the public life of Social Media Data. *Social Media + Society*, *6(2).* doi.org/10.1177/2056305120915618

Hartung, P. (2020, Nov.). The children's rights-by-design standard for data use by tech companies. *UNICEF.* unicef.org/globalinsight/media/1286/file/%20UNICEF-Global-Insight-DataGov-data-use-brief-2020.pdf

LastPass. (n.d.). Why LastPass. lastpass.com/why-lastpass

Leizerov, S. (2000). Privacy advocacy groups versus Intel. *Social Science Computer Review*, *18*(4), 461–483. doi.org/10.1177/089443930001800409

Madden, M., and Rainie, L. (2015, May 20). Americans' attitudes about privacy, security and surveillance. *Pew Research Center*. pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

Msughter, A.E. (2020). Internet Meme as a Campaign Tool to the Fight against Covid-19 in Nigeria. *Global Journal of Human-Social Science. 20*(6).

Nakashima, R. (2018, Aug. 13). Google Tracks your movements, like it or not. *AP News*. apnews.com/article/north-america-science-technology-business-ap-top-news-828aefab64d4411bac257a07c1af0ecb

Newell, J. (2013, Oct 26). Thousands gather in Washington for anti-NSA 'stop watching us' rally. *The Guardian*. theguardian.com/world/2013/oct/26/nsa-rally-stop-watching-washington-snowden

r/privacy. Reddit. (n.d.) reddit.com/r/privacy

r/privacyguides. Reddit. (n.d.). reddit.com/r/PrivacyGuides/

Simko, Chang, Jiang, Calo, Roesner, and Kohno. (2022). Covid-19 contact tracing and privacy: A longitudinal study of public opinion. *Digital Threats: Research and Practice*, *3*(3), 1–36. doi.org/10.1145/3480464

Snapchat. (2023, April 19). Say hi to My AI … (Twitter). twitter.com/Snapchat/status/1648748425494790144

Snowden, E. (2014). Here's how we take back the Internet [Video]. TED Conferences. ted.com/talks/edward_snowden_here_s_how_we_take_back_the_internet/transcript?language=en

Sun, Sugatan, Afnan, Simon, Gelman, Radesky, and Schaub. (2021, May 7). "they see you're a girl if you pick a pink robot with a skirt": A qualitative study of how children conceptualize data processing and digital privacy risks. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. doi.org/10.1145/3411764.3445333

Tao, J., and Shuijing, H. (2016). The elderly and the big data how older adults deal with Digital Privacy. *2016 International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS)*. doi.org/10.1109/icitbs.2016.35

TheDayWeFightBack.org. (2014). Today, February 11th, 2014 Is The Day We Fight Back Against Mass Surveillance. thedaywefightback.org/

Tor Project (2021). 2021 Annual Report. torproject.org/static/findoc/2020-2021-TorProject-Annual-Report.pdf?h=3fdc0ff6.

u/cryotosensei. (2023, Feb 13). 5 reasons why I love Nostr. Reddit.com. reddit.com/r/nostr/comments/111di02/5_reasons_why_i_love_nostr/

United States v. Carpenter et al. (2015). Brief of amici curiae American Civil Liberties Union, American Civil Liberties Union of Michigan, Brennan Center for Justice, Center for Democracy & Technology, Electronic Frontier Foundation, and National Association of Criminal Defense Lawyers in support of defendants-appellants seeking reversal in *United States v. Carpenter et al,* 14-1572 & 14-1805 (United States District Court for the Eastern District of Michigan, Southern Division, 2015)

United States v. Hamilton (2012). Brief of amicus curiae Electronic Privacy Information Center (EPIC) in support of appellant and urging reversal in *United States v. Hamilton*, 11-4847 (4th Cir. 2012)

van Dijck, J. (2013). ‘you have one identity’: Performing the self on Facebook and linkedin. *Media, Culture & Society*, *35*(2), 199–215. doi.org/10.1177/0163443712468605

Veritone. (2022, Nov. 30). *Intelligent audio, Image and Video evidence redaction software*. Veritone. veritone.com/applications/redact/

Wäscher, T. (2016). Framing resistance against surveillance. *Digital Journalism*, *5*(3), 368–385. doi.org/10.1080/21670811.2016.1254052

White, J. (2021, Feb. 4). Yahoo announces 500 million users impacted by Data Breach. LifeLock by Norton. lifelock.norton.com/learn/data-breaches/company-data-breach#

Zimmer, M. (2014, February 3). Mark Zuckerberg's theory of privacy. *The Washington Post*. washingtonpost.com/lifestyle/style/mark-zuckerbergs-theory-of-privacy/2014/02/03/2c1d780a-8cea-11e3-95dd-36ff657a4dae_story.html