Advocating for Privacy when Personal Information Is Currency

A Sociotechnical Research Paper
presented to the faculty of the
School of Engineering and Applied Science
University of Virginia

by

Karim Shoorbajee

April 5, 2021

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.

Karim Shoorbajee

***Sociotechnical advisor*:** Peter Norton, Department of Engineering and Society

Preface

Software can better serve its human users.

Video games often include non-playable characters and opponents controlled by Artificial Intelligence. A proposed AI unit was developed for incorporation into CS 4730. It explains what AI is in games and covers things like enemy/npc AI and AI in virtual tabletop games. The proposal includes a week's worth of material to be taught in this unit and how it will fit into the course as it is. It also includes examples of homework based in the Unity game engine that would be completed alongside the instruction. Well programmed AI makes games more balanced, immersive, and enjoyable. Modern games are utilizing increasingly complex and believable AIs so an AI unit is of great importance to a game design class.

the United Nations' Universal Declaration of Human Rights states "No one shall be subjected to arbitrary interference with his privacy... Everyone has the right to the protection of the law against such interference or attacks." How do internet users advocate for their personal privacy against companies that rely on selling user information to advertisers to make revenue (e.g. Facebook and Google)? Internet users have advocated for their privacy by arguing they should be compensated for their data, declaring privacy as a human right, using technology that protects their privacy, and advocating against intrusive company data policies.

Advocating for Privacy when Personal Information Is Currency

Social media companies' business model is to collect user data and monetize it by using it to target advertisements. Social media users pay for these companies' services by forfeiting their personal information, which grants social media companies much power. Former Google design ethicist Tristan Harris stated, "If I have data, then I know exactly what's going to move [a user's] psychology, and I can persuade your mind in ways that you wouldn't even know were targeted just at you" (Thompson, 2017).

Social media is pervasive worldwide. Most Americans use Facebook and YouTube; most young Americans use Snapchat and Instagram (Smith and Anderson, 2018). The United Nations' Universal Declaration of Human Rights states "No one shall be subjected to arbitrary interference with his privacy... Everyone has the right to the protection of the law against such interference or attacks." This raises the question: how do internet users advocate for their personal privacy against companies that rely on selling user information to advertisers to make revenue (e.g. Facebook and Google)?

Nonprofits such as the Electronic Privacy Information Center (EPIC), Consumer Federation of America (CFA), and the American Civil Liberties Union (ACLU) are strong advocates of digital privacy. Individual social media users who value privacy take their own action to maintain online privacy. These groups' agendas are at odds with social media companies such as Facebook, Google, and Snapchat. Internet users have advocated for their privacy by arguing they should be compensated for their data, declaring privacy as a human right, using technology that protects their privacy, and advocating against intrusive company data policies.

Review of Research

Best and Pane (2018) provide a framework for how students' privacy can be protected in the advent of digital education systems: "Developers must find ways to meet [privacy and data security] expectations while also staying abreast of changes to policy and regulation. Mechanisms must be put into place to protect privacy and enable use of education technology data within the acceptable bounds." O'Connor (2015) gives examples of policies that should be implemented in the United States to protect privacy in the digital age (pp. 25-27). She states "The government is responsible for setting reasonable limits on data collection and use in order to empower all users equally," but doesn't describe how privacy advocates fight for this legislation.

Warren and Brandeis (1890) discuss, early on, the need for comprehensive privacy protections along with technological developments. They discuss the development of consumer grade cameras and sensationalized press stating these inventions "Have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.' For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons." Devries (2003) presents the challenges of ensuring privacy in the digital age including "Collection of vast amounts of personal data..., the globalization of the data market… and lack of the types of control mechanisms for digital data that existed to protect analog data." This research helps explain the growing privacy concerns amongst internet users, and why there have been a variety of efforts from them to protect privacy.

Personal Information as a Commodity

Advocates of internet privacy have argued that their personal information should be treated as a commodity and they should be compensated for it justly. Computer scientist Jaron Lanier proposes a system where social media companies pay users for the data they collect and charge users a small premium for their services: “You'll get paid for your data and more than you think plus you'll pay for services that are free now but in the balance you'll do better” (Lanier, 2019). Lanier claims under his system, social media companies and advertisers will be disincentivized in using personal data in manipulative ways: “Because using your own data against you will cost money any company… will be dissuaded from doing that. Instead they'll come up with productive creative things to do where they add value.” Research conducted by internet technology company Twingate concluded that internet users are willing to pay far more than the revenue their data generates for social media companies to not sell their data (Twingate, 2020). Internet users have opted to use apps like UBDI (Universal Basic Data Income) where they get paid to share their data. UBDI “Helps people make money by sharing anonymous insights from their data that companies need for market research” (UBDI, n.d.). There’s a clear movement amongst advocates of digital privacy to stop forfeiting their data to technology companies without compensation.

Privacy as a Human Right

Other advocates of data privacy argue for their privacy treated not as a commodity but as a human right. Susan Grant, Director of Consumer Protection and Privacy at the CFA states “What [internet users] are demanding is rights in regard to that data… and the right to be able to hold companies accountable for violating their privacy.” In Davis vs. Facebook (2017) of the US

9th Circuit Court, plaintiffs accused Facebook (a California-based company) of collecting users' sensitive medical data. They argued Facebook's actions violate Article 1 of the California Constitution which provides "All people… have inalienable rights. Among these are… pursuing and obtaining… happiness, and privacy" (California Constitution Article I. Section 1). Plaintiffs reasoned "The phrase 'and privacy' was not added until 1972…. the 'primary purpose' of adding these two words was 'to afford individuals some measure of protection against'... 'unnecessary information gathering . . . [by] computer stored and generated 'dossiers,'" (Smith vs. Facebook, 2017). Plaintiffs made a similar argument in a 9th Circuit appealed case concerning Facebook's practice of tracking internet users who don't have Facebook accounts (Davis vs. Facebook, 2017). With over one million subscribers, r/Privacy is a Reddit forum focused on maintaining privacy in the digital age. Their FAQ states "We must retain some control over how information about us is collected and used. Privacy is a human right which is intimately linked with our many notions of freedom" (r/Privacy, n.d.) Advocates of internet privacy have routinely argued for their privacy as a human right, and accused social media companies of violating it.

Cross Site Tracking

Internet users use software and technology that combats information gathering and selling. A primary way social media companies target advertisements is by tracking individuals' usage patterns via cookies (pieces of information a website can store on a user's browser). Social media companies even employ cross site tracking cookies that can surveil usage after they leave the website, or if they don't have an account on that website at all (Mozilla, 2018). Because of this, users choose to use browsers with more defensive cookie storage policy. Katherine Schwab of Fast Company states "Chrome allows third-party websites to access… any information that

site has tracked using cookies. If you care about privacy at all, you should ditch the browser that… [enables] other companies to track your online movements… for one that does not use your data at all" (Schwab, 2018). She then explains that she switched to using Firefox for its tracker blocking. Aquil Roshan of It's FOSS encourages users to switch to Firefox stating "Google… wants you to pay [for Chrome] with your personal data. It wants to snoop, spy and stalk you... Firefox does not send your private info to its servers or any third-party partners" (Roshan, 2020). Privacy conscious internet users are switching to other browsers too. Gary Sims of Android Authority switched to Brave stating "Most advertising platforms use techniques to try to identify you and track you as you move across the web. Brave browser blocks all this, allowing you to browse freely" (Sims, 2021).

Internet users have also opted for more private search engines, as leading engine Google uses search behavior to sell ads. Bradley Chambers of 9to5mac states "If you want excellent search results that aren't used to target you with better ads, use DuckDuckGo... I've decided that protecting my privacy is a worthy trade-off for slightly worse search results" (Chambers & Chattanooga, 2021). R/Privacy also encourages its users to use DuckDuckGo as it "Has a well formed and reasonable privacy policy" (r/Privacy, n.d.).

Some advocates argue that government action needs to be taken against companies that use cross site tracking. Jeffrey Chester of the Center for Digital Democracy addresses developments in Google's cross site tracking abilities stating "It was the failure of regulators to rein in this industry over the years that led to the current crisis… That's why we call on the Biden Administration, the FTC and the Congress to investigate these proposed new approaches for data use" (Chester, 2021). Bennett Cyphers of the Electronic Frontier Foundation sheds light on the overwhelming presence of Google on the internet (their large share of the browser market

and almost unanimously used web applications) and how Google aggregates data through its services to sell to advertisers with users unable to opt out. They state this "Underscores the need for a more comprehensive law that treats privacy as a default, not an option" (Cyphers, 2020). Advocates use cross site tracking as grounds to fight for data privacy legislation.

Data Misconduct

Advocates of internet privacy respond to data misconduct by internet companies to argue for laws and regulations to protect internet users' privacy. Data analytics company Cambridge Analytica created a quiz on Facebook under research pretext but used data from the quiz to target ads in aid of the 2016 Trump campaign. EPIC wrote to the FTC that this violated a 2011 FTC order that protected Facebook users' data from third party apps: "Facebook's transfer of personal data to Cambridge Analytica was prohibited by the 2011 Facebook Order… The Commission must immediately undertake an investigation and issue a public report as to whether Facebook complied with the 2011 Order" (EPIC et al, 2011). This letter was cosigned by other action groups including the CFA. California legislators unanimously passed The California Consumer Privacy Act which makes more transparent the data companies collect against consumers. The statute includes "It came to light that tens of millions of people had their personal data misused by… Cambridge Analytica… As a result, our desire for privacy controls and transparency in data practices is heightened" (California State Legislature, 2018). In response to the Equifax Data Breach of 2017, EPIC proposed reforms to protect consumers' data including enacting the Consumer Privacy Bill of Rights, legislation that was drafted during the Obama administration "that would put the responsibilities on companies that collect and use personal data to protect the information they choose to collect" (EPIC, 2017).

Notice and Choice

Advocates of online privacy bring to light convoluted social network privacy policies. They accuse social media companies of giving users the illusion of control over their data. Many social media companies employ a "notice and consent" model for disclosing privacy policy. Brian Kint of Cyber Law Monitor challenges "notice and consent" as adequate privacy protection stating "Privacy notices are often buried in terms of service that are lengthy, confusing, and difficult to read... The term 'privacy notice' may give users the impression that it contains information on how the organization is going to protect personal information rather than how it is going to disclose that information, which further disincentives a close read" (Kint, 2019). Kint's assertions are corroborated by Florencia Marotta-Wurgler's paper on website privacy policies. She analyzes 248 privacy policies (many of which are social media sites) and concludes "The general assessment [on notice and consent] is not favorable… The substance of the rights that are explicitly reserved are sometimes fairly concerning." When commenting on their length and language she states "It's just very hard to get a clear meaning from them" (Marotta-Wurgler, 2015).

In a letter to the US Committee on Energy & Commerce, EPIC pushes for digital privacy legislation. In their contingency titled "Individual rights (right to access, control, delete)" they state, "Notice and consent has little to do with privacy protection. This mechanism allows companies to diminish the rights of consumers, and use personal data for purposes to benefit the company but not the individual" (EPIC, 2019). EPIC has argued for data minimization as an alternative to notice and choice, stating that it is "More effective at protecting the confidentiality of consumer data than notice and choice… Research by FTC Chief Technologist Lorrie Cranor

correctly summarized the benefits of data minimization: 'If there is less data to transmit and protect, there is less chance of unauthorized access'" (EPIC, 2016).

In a US House Committee on Energy & Commerce hearing titled "Protecting Consumer Privacy In the Era of Big Data" president of the Center for Democracy and Technology (CDT), Nuala O'Connor criticizes the status quo of internet privacy policies: "The sheer number of privacy policies, notices, and settings or opt-outs one would have to navigate is far beyond individuals' cognitive and temporal limitations." She goes on to request specific legislation which should "Provide individual rights to access, correct, delete, and port personal information; require reasonable data security and corporate responsibility; prohibit unfair data practices…; prevent data-driven discrimination and civil rights abuses" (O'Connor, 2019).

Organizations and individuals are critical of the notice and choice, status quo approach to privacy policy and use it as a launching point to advocate for stronger data protection laws and practices.

Biometric Information

Advocates of data privacy are critical of social networks' collection of biometric data and use this to call for stricter data protection. In 2011 Facebook, without notifying its users, automatically suggested individuals to be tagged in photos. This implied when users manually tagged their friends in photos, Facebook was aggregating images of users' faces to automatically detect their presence in future photos. A LA Times Oped includes, "The system encourages people even more strongly to disclose information about others who might not welcome the exposure… What it really should have done, though, was ask them to opt in instead of merely, quietly, giving them a way out." They voice concerns about the harboring of mass amounts of

facial data stating “A larger concern is what Facebook may eventually do with its growing collection of facial images — for example, how it might make the technology available to advertisers” (Los Angeles Times, 2011). EPIC filed a complaint against the FTC, cosigned by The Center for Digital Democracy and Consumer Watchdog, criticizing Facebook’s actions and calling on the Commission to take action: “This representation of biometric information, based on the user’s facial image, generated by Facebook, is available to Facebook but not to the user.” They describe the lengthy and confusing process for someone to have Facebook delete their biometric information. They describe Facebook’s practice as an invasion of privacy and call on the FTC to enforce stricter privacy regulations on Facebook. Included in EPIC’s requests is “Require Facebook to establish… a comprehensive privacy program… to address privacy risks related to the development and management of new and existing products and services for consumers, and protect the security, privacy, confidentiality, and integrity of consumer information” (EPIC, 2011).

In Patel v. Facebook (2018) plaintiffs argued Facebook’s Tag Suggestion tool (as described above) violates Illinois Biometric Information Privacy Act (BIPA). The ACLU filed an amicus brief supporting the plaintiff’s right to sue and argues for the upholding of BIPA as important protection for internet users against poor privacy practice. They argue “Without reasonable limits, biometric technologies enable corporations… to pervasively track people… in public and private spaces.... Only with enforceable protections of the kind enshrined in BIPA can society hope to mitigate those risks” (ACLU, 2018).

Conclusion

The fight for privacy in the internet age is in a race against the quickly augmenting technologies that power our online world. People's value of privacy protection in the United States dates as early as the 4th amendment of the Constitution, but this hasn't been enough time to strike a balance between the companies that collect our data and the individuals who use their services. This is due to the constant evolution of technology; in this context, biometric information collection, cross-site tracking, and mass data collection by internet companies. Tech companies' business model drives the conflict. If these companies didn't need to sell user information to be profitable, there would be less conflict regarding their data practices.

The advocacy for privacy against technology companies can be broken into two main strategies: There are activist groups and organizations who spread awareness about privacy concerns in the digital age and push for policy change, and individuals who fight for their privacy on an individual basis through their behaviors and choices as consumers. Groups like EPIC, ACLU, CFA, CDT and others put a lot of effort into advocating for privacy legislation that benefits the consumer. They also take great interest in court cases and legal disputes regarding technology companies' data management. Meanwhile it's evident there are actions individuals can take to protect their own privacy. They can use software that protects their data, or avoid using certain services at all. Also, advocates of personal privacy are not in agreement as to what strategies should be taken to protect consumers. We obviously need to give social media sites some of our information for them to function properly. Whether we should require social media sites to collect and use our data as little as possible (data minimization) or just be compensated for the data we give is an open debate.

Individuals have fought against cross site tracking through blocking cookies, but social media companies are too clever for that to stop their information gathering. The development of browser fingerprinting allows for websites to track individuals without using cookies. Fingerprinting is much harder to combat as it is based on an individual's computer specifications and browser settings (Taylor, 2021) whereas cookies are files an individual can delete on their computer. Further research could assess how participant groups have fought to combat this new data collection process.

References

ACLU. (2018, December 17). In Re Facebook Biometric Information Privacy Litigation. Carlo Licata, Nimesh Patel & Adam Pezen, https://epic.org/amicus/bipa/patel-v-facebook/Patel-v-FB-9th-Cir-ACLU-Amicus.pdf

California Constitution. Art. I, Sec. 1.

California State Legislature. (2018, June 29). Assembly Bill No. 375 https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

Chambers, B., & Chattanooga, B. (2021, February 09). DuckDuckGo: Why I switched to it from Google search.https://9to5mac.com/2021/02/09/duckduckgo/

Chester, J. (2021, February 18). The whole world will still be watching You: Google & digital marketing. https://www.democraticmedia.org/article/whole-world-will-still-be-watching-you-google-digital-marketing-industry-death-cookie

Cyphers, B. (2020, July 10). Google says it Doesn't 'sell' your Data. Here's how the company Shares, Monetizes, and exploits it. https://www.eff.org/deeplinks/2020/03/google-says-it-doesnt-sell-your-data-heres-how-company-shares-monetizes-and

DeVries, W. (2003). Protecting Privacy in the Digital Age. Berkeley Technology Law Journal, 18(1), 283-311. April 4, 2021, http://www.jstor.org/stable/24120519

EPIC. (2011, June 10). EPIC's FTC Complaint in In re Facebook and Facial Recognition. https://epic.org/privacy/facebook/EPIC_FB_FR_FTC_Complaint_06_10_11.pdf

EPIC. (2016, November 7). Standards for Safeguarding Customer Information Request for Public Comment. https://www.ftc.gov/system/files/documents/public_comments/2016/11/00030-129356.pdf

EPIC. (2017). Equifax Data Breach. https://epic.org/privacy/data-breach/equifax/

EPIC. (2019, October 29). EPIC to Congress: Reauthorize SAFE WEB Act, Pass Federal Privacy Law. https://epic.org/2019/10/epic-to-congress-reauthorize-s.html

EPIC et al. (2018, March 20). Coalition Letter Urging FTC to Investigate Facebook [Letter written March 20, 2018 to FTC]. https://www.epic.org/privacy/facebook/EPIC-et-al-ltr-FTC-Cambridge-FB-03-20-18.pdf

Kint, B. (2019, February 13). Is it time to rethink notice and choice as a fair information privacy practice? from

https://www.cyberlawmonitor.com/2019/02/13/is-it-time-to-rethink-notice-and-choice-as-a-fair-information-privacy-practice/

Lanier, J. (2019, Sept. 23). Jaron Lanier Fixes the Internet. New York Times. https://www.nytimes.com/interactive/2019/09/23/opinion/data-privacy-jaron-lanier.html

Los Angeles Times. (2011, June 11) “Facebook’s Face Problem.” Los Angeles Times, www.latimes.com/opinion/la-xpm-2011-jun-11-la-ed-facebook-20110611-story.html.

Marotta-Wurgler, F. (2015, April). Does “Notice and Choice” Disclosure Regulation Work? An Empirical Study of Privacy Policies (Rep.). https://www.law.umich.edu/centersandprograms/lawandeconomics/workshops/Documents/Paper13.Marotta-Wurgler.Does%20Notice%20and%20Choice%20Disclosure%20Work.pdf

Mozilla. (2018, April 12). Cross-site tracking: Let's unpack that. https://blog.mozilla.org/firefox/cross-site-tracking-lets-unpack-that/

O'Connor, N. (2019, February 26). Statement of Nuala O’Connor, President and CEO, Center for Democracy & Technology. https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Testimony_Nuala O'Connor 02.26.2019.pdf

O'Connor, N. & Lange, A. (2015). Privacy in the Digital Age. Great Decisions, 17-28. http://www.jstor.org/stable/44214790

r/Privacy. “Privacy & Freedom in the Information Age.” Reddit, www.reddit.com/r/privacy/wiki/index#wiki_what_can_i_do_to_protect_my_privacy.3F

Best, K., & Pane, J. (2018). (Rep.). RAND Corporation. doi:10.2307/resrep19899

Schwab, K. (2018, July 10). Bye, Chrome: Why I'm switching to Firefox and you should too. http://www.fastcompany.com/90174010/bye-chrome-why-im-switching-to-firefox-and-you-should-too

Smith, A., & Anderson, M. (2018, March 1). Social Media Use 2018: Demographics and Statistics. Pew. https://www.pewresearch.org/internet/2018/03/01/social-media-use-in-2018/

Sims, G. (2021, January 26). Should you switch to the brave web browser? http://www.androidauthority.com/brave-browser-review-1110069

Taylor, S. (2021, March 09). Browser fingerprinting (explanation, tests, and solutions). https://restoreprivacy.com/browser-fingerprinting/

Thompson, N. (2017, July 26). Social Media Has Hijacked Our Minds. Click Here to Fight It. Wired.

https://www.wired.com/story/our-minds-have-been-hijacked-by-our-phones-tristan-harris-wants-to-rescue-them/

Twingatehq. “Internet Security Research - Privacy for a Premium.” Twingate, 17 May 2002, www.twingate.com/research/privacy-for-a-premium-exploring-peoples-sentiments-on-paying-for-social-media/

UBDI. It's Time for Universal Basic Data Income, www.ubdi.com/individuals/how-earning-works.

United States Court of Appeals for the Ninth Circuit. On Appeal from the United States District Court for the Northern District of California. Davis vs. Facebook. 18 Sept. 2017, https://epic.org/amicus/facebook/davis/Davis-v-Facebook-Plaintiffs-Brief.pdf

United States Court of Appeals for the Ninth Circuit. On Appeal from the United States District Court for the Northern District of California. *Smith vs. Facebook.* 18 Sept. 2017, www.epic.org/amicus/facebook/smith/Smith-Opening-Brief.pdf

Warren, S., & Brandeis, L. (1890). The Right to Privacy. Harvard Law Review, 4(5), 193-220. doi:10.2307/1321160