Is Privacy Dead? The Cost of Convenience: A Narrative Review

by

Emmanuel DeJesus Jr.

BS, University of South Carolina Aiken, 2019

MS, Western Governor's University 2021

A Research Paper Submitted to the School of Computing Faculty of

Middle Georgia State University in

Partial Fulfillment for the Requirements for the Degree

DOCTOR OF SCIENCE IN INFORMATION TECHNOLOGY

MACON, GEORGIA
2024

Is privacy dead? The cost of convenience: A narrative review

Emmanuel DeJesus Jr., *Middle Georgia State University, emmanuel.dejesus@mga.edu*

Abstract

In the United States, technology has become deeply integrated into all facets of daily life, resulting in a significant increase in data collection. This study undertakes a comparative analysis of peer-reviewed articles and legislative documents about user privacy and convenience. It identifies several emerging themes, provides examples, and discusses potential legislative changes and improvements.

Keywords: Privacy, convenience, information technology, graduate studies

Introduction

Technology and life have harmoniously intertwined in recent years, bringing unparalleled convenience and connectivity, but has led to an erosion of privacy (Obar & Oeldorf-Hirsch, 2020). More tracking technology and data collection points exist on roads, grocery stores, and airports than ever before, and people continue to share their personal information with these digital cities. The ubiquity and convenience of digital devices leave people no choice but to become a digital part of their surroundings (Eckhoff & Wagner, 2017). The same tools and platforms that enhance our lives have also become repositories for an unprecedented amount of personal data. That data raises profound questions about the sanctity of personal information and the benefits of technological progress compared to digital convenience.

Utilizing a narrative review modeled after Jones (2004), the study traces privacy legislation, identifying key legislative milestones and the regulatory responses they have elicited. This in-depth analysis of peer-reviewed articles, coupled with legislation, provides a holistic understanding of the contentious relationship between the rapid advancements in technology and the efforts to safeguard individual privacy.

Two questions can be thought of for analysis: What reasons do users forfeit their privacy, and is it possible that American privacy legislation adds to that forfeiture of digital privacy? This study explores possible themes emerging from the literature to provide reasoning for consumer behavior while examining current legislation for adequate protection of American digital privacy.

Merging literature and law in one study for American digital privacy allows the research to illuminate prevalent contemporary issues while offering untrodden advancements in repairing the digital divide. In doing so, it supplements the already rich conversation on convenience and digital privacy by inquiring about what is lost in a race toward convenience.

Problem Statement

The ubiquity of digital devices and widespread data collection in our daily lives introduce a plethora of privacy concerns in the name of convenience. Technological advances place a strain on the privacy rights of the individual and leave people no choice but to become a digital part of their surroundings (Eckhoff & Wagner, 2017). Data collection coupled with a weak legislative framework that wrestles with expeditious digital evolution raises profound questions on digital privacy in the modern age.

The European Union (EU) has established a vanguard in the realm of digital privacy by developing the General Data Protection Regulation (GDPR) (Gilman, 2020). The United States, while following suit in forging regulation regarding digital privacy initiatives, only has laws in a few states. The most notable of the states that developed laws is California, and it is called the California Consumer Privacy Act (CCPA) (Bonta, 2023). A complete comprehensive legal framework for the United States remains to be seen. A lack of cohesive rulings protecting these rights may proliferate and become a model for the future of technology instead of an inviolable digital right.

Purpose

The modern digital landscape has revolutionized the way we share and access information, but do people know how much and what is being shared about their personal information? The purpose of this research is to investigate legislation related to privacy and convenience and examine its impact on security and privacy. This study seeks to understand the relationship between consumer privacy, their sacrifices and convenience and current legislation. This study aims to discover themes that emerge from the literature to chart a new course for digital rights and privacy legislation. If a balance can occur between the disparate issues of digital privacy and American privacy legislation, personal data may not be required as a currency of convenience.

Research Questions

This study addresses the following questions regarding privacy and convenience:

RQ1: What major themes emerge from the literature regarding consumer privacy sacrifices?
RQ2: Are changes required in American privacy legislation?

Objectives

This research aims to illuminate how individuals forfeit their digital rights in the modern age and to identify the factors that drive these concessions.

Review of Literature

When addressing privacy, one must be cognizant of the laws both foreign and domestic. In the United States (US) there is no one privacy policy in effect. However, The US has a few states that have ratified acts or are considering privacy policies, such as California, Virginia, Colorado, New York and Washington. There is a gap in the coverage of privacy laws within America (Bonta, 2023). If only five states produced extensive privacy laws, then most Americans within the country live with zero protection. California has six privacy rights detailed for consumers according to the California Consumer Protection Act (CCPA) (Bonta, 2023). The rights listed within the CCPA are the right to know, the right to delete, the right to opt out, the right to correct, and the right to limit. There are limits to the code that require users to understand what they are asking of a company and cannot make unreasonable demands.

In the CCPA is the right to know (Bonta, 2023). A consumer's right to know allows individuals to understand how information is being collected and how it is being used and shared. The right to delete gives consumers the authority to delete information that has been collected about them. The right to opt-out provides users the ability to refuse the sale or sharing of their personal information. An interesting right provided by the CCPA is the right to correct. If a user allows the collection of information, they have the right to make sure all information that is being shared by a business is accurate. Lastly, the right to limit administers the right to the consumer to limit the use and disclosure

of their sensitive information. It should be stated that some of these rights have caveats and exceptions, but most laws work this way.

The first comprehensive law for privacy existed back in 1995, called the Data Protection Directive, but it was not enforced or complied with (Hoofnagle et al., 2019). Fast forward 16 years a successor was born that defends privacy for all the European Union regardless of where the data is processed. The EU requires that if business is done or a webpage is served to residents of the EU, they must know what is collected and can opt in or out of the data collection. The document for the EU is called the General Data Protection Regulation (GDPR) (General Data Protection Regulation, 2023). This document entails the same details as the CCPA for the most part, except it has a right called "the right to be forgotten". GDPR as a regulation was widely accepted by the EU residents, and this is what sparked the change in the United States. A right to be forgotten means that a consumer can request their information be deleted and all copies or replicates must be erased. Ashley (2020) explains that companies must make it easy for consumers to revoke consent at any time. GDPR also extends to any companies that operate within the EU. While the protections for the EU extend far and wide it only applies to those countries within the EU and places like Africa do not receive coverage by the body of law.

Privacy has long been a topic of concern. One of the first influential essays on privacy dates back to 1890 and was written by Samuel Warren & Louis Brandeis. The authors of the article focused on the idea of "the right to be let alone," which is still referenced to this day (Warren & Brandeis, 1890). It can be argued that the right to be, let alone helped promote the idea of "the right to be forgotten". Privacy itself is not a simple concept and is fluid. The idea changes with the concepts of people and their respective times. Westin (1966) argued two points in his paper. The first is that an individual should not have information given for one purpose and use it for another without their consent. This same thought is observed within the CCPA's right to opt-out and right to know. Interestingly, arguments made over sixty years ago endure the test of time. The second is that an individual should have the capability to decide for oneself what information can and will be exposed to the public. The resulting right borrowed by the CCPA is the right to opt-out.

Much like today, privacy continues to be argued over, but it has not changed much. Technology has added a new layer of complexity to the topic of privacy that cannot be undone. Privacy policies and frameworks are built not as a checklist item but as a powerful social norm based on peoples' expectations, not corporations (Krupp, 2022). The policies that are put in place should reflect the population's feelings towards the subject and not the money that is exchanged between enterprises and governments; that idea from the reading suggests the push for governmental regulation such as the CCPA and GDPR by leveraging heavy fines.

An End User License Agreement (EULA) is a document that states a product's terms and conditions written by the company. A EULA can often incorporate a wide variety of contract provisions, including terms of use, privacy notices and cookie policies (Ericson et al., 2022). EULAs are the agreements consumers agree to when they install a new product with their installation that tends to get overlooked. No law requires companies to incorporate a EULA but adding one is a best practice for organizations to protect themselves from possible lawsuits. According to an experimental study of a fake social networking site, 98% of 543 participants missed clauses of sharing data with the NSA and employers as well as giving up their firstborn child as payment within the EULA (Obar & Oeldorf-Hirsch, 2020). The same study explains that people would not read the information because it was "too long" or all the policies are "the same" or they could not "understand it". The first two reasonings for skipping rest on the people who overlooked it and their security awareness, but the last reasoning suggests something else entirely. A user who does not understand it suggests a discrepancy between the law and corporations' policies regarding their services.

To understand what collects data when perusing the internet, a cookie needs to be defined. Cookies are files that contain small pieces of data when browsing the internet (Aziz & Telang, 2016). The data that is collected by websites can be used to track users. Cookies enable ad agencies to track users' browsing behavior by identifying which pages are visited and for how long, what is clicked, and even what is purchased (Aziz & Telang, 2016). The mandates discussed help users opt out of when cookies are collecting data and what data is being collected. Cookies are an important piece of understanding how the web works and can shed light on the inner workings of search engines. To give a complete picture of what is and what can be tracked, Ashley (2020) reveals virtually limitless information can be obtained, such as physical health, mental health biometric data, social networks, daily routine, and preferred news organizations. Since only a few states have privacy rulings in place similar to CCPA, that means the rest of Americans do not get to opt out of data collection like the ones voiced. In the end, the legal documents such as the EULA, privacy policy, and even cookies that one agrees to when using a website are developed for transparency and have become more important after the introduction of GDPR and CCPA legislation. The laws explained are great for protecting constituents; however, what they excel in is providing people with security awareness of what they are conceding out of convenience.

In sum, the literature reveals a complex landscape of privacy rights and protections, characterized by fragmented US laws and more comprehensive regulations in the European Union. The ongoing dialogue on privacy underscores the need for a balanced approach that respects individual rights while accommodating technological innovation.

Methodology

This study employs a narrative review method (Jones, 2004) to systematically evaluate and integrate findings from peer-reviewed articles, legal documents, and authoritative texts concerning privacy, technology, and the impact of legislative measures. This approach facilitates a comprehensive understanding of the progressing dialogue around privacy rights in the digital age, emphasizing the intersection between technological convenience and legislative responses.

Data Collection Procedure

A meticulous selection process was endured to compile the relevant and detailed literature. The process focused on works published within the last two decades (2003-2023) to ensure the relevance of the data and information provided. The only exception to this criterion was historical documents pivotal for context, such as foundational privacy legislation or landmark scholarly contributions to the field of privacy rights.

The literature was sourced from an array of academic databases, including Google Scholar, IEEE Xplore, JSTOR, and ProQuest Research Library, leveraging college-funded access to e-books, research papers, peer-reviewed journals, and case studies. Keywords instrumental in refining the search encompassed terms like "erosion of privacy," "security vs. privacy," "GDPR," and "privacy policy." Boolean search strategies using "AND" and "OR" were utilized to broaden the scope of the search and capture a diverse range of relevant literature.

Data Acquisition and Analysis

Selected articles underwent a thematic analysis (Jones, 2004) to identify and categorize emerging themes related to legislation, security awareness, and technological data collection. This analysis was

informed by the framework proposed by Braun & Clarke (2006), undergoing an iterative process of familiarization, theme generation, coding, and thematic assessment.

The initial phase involved developing a deep familiarity with the collected data, focusing on historical and contemporary legislation surrounding privacy, data collection methods, and consumer policy. Following the initial phase, themes were generated to encapsulate the overarching narratives within the literature, and many examples and detailed explanations were provided to support the narratives in the context of privacy.

Coding was applied to systematically categorize the literature according to identified themes, facilitating a structured comparison and analysis. This step is the evidence collected and its respective categories, fulfilling the study's objectives. Fifteen key articles were used in the narrative review as displayed in Table 1; the literature was grouped into 4 distinctive themes. The 4 emerging themes are: (1) gaps in law, (2) speed, (3) perception of security awareness, and (4) services in technology.

Table 1: Theme, Reference, and Contribution

Theme	Authors	Contribution
1	Warren, D. S., & Brandeis, D. L. (1890).	Background of where privacy started in America
1	Westin, F. A. (1966).	Continuation of how privacy progressed in American society
1	General Data Protection Regulation. (2023).	EU legislation passed in 2018 sparking a digital change in America
1	Amnesty International. (n.d.).	Understanding of where America stood with digital privacy
2	Abdulghani, A. H., Nijdam, A. N., & Konstantas, D. (2022).	How convenience can give away location data
2	Dooley, R. (2023, November 28).	Subcutaneous scanning going on in public places
2	Obar, J. & Oeldorf-Hirsch, A. (2020).	Users choose speed regardless of pervasive technology
3	Kim, C. B., & Park, W. Y. (2012).	Society chooses the dominant option rather than a dominant product
3	Schneier, B. (2015).	Study on how fear causes acceptance of privacy invasions
3	Stecklow, S., Cunningham, W., & Jin, H. (2023, April 6).	Findings on Tesla recordings and privacy violations
3	Yerby, J., & Floyd, K. (2018).	Study on security awareness of users
3	Yerby, J. & Vaughn, I. (2022).	Argues a need for readable contracts for users to accept
4	Ozeran, L., Solomonides. A., & Schrieber. R. (2021).	Explains users are willing to give up data if it appears they gain from it
4	Indrayani, I., & Maharani, T. (2022).	Explanation of when consumers accept a service they divulge information

4	Gerber, N., Gerber, P., & Volkamer, M. (2018).	Consumers will give up data if they believe they can win a prize

1 = gaps in law; 2 = speed; 3 = perception of security awareness; 4 = services in technology.

The thematic analysis culminated in a discussion on the state of privacy and legislation in the United States, explaining weaknesses, exploring changes and strengths. The findings from this analysis provided a foundation for discussing the implications of identified themes and contemplating future directions for enhancing privacy protections.

Results

Within the last 10 years, groundbreaking legislation has reared its head surrounding privacy. GDPR gained traction and was enforceable compared to the Data Protection Directive because of its fines of 8 figures to enterprises that fail to comply (Hoofnagle et al., 2019). The push for new privacy legislation around the world allowed for statewide privacy legislation to proliferate in the states, starting with CCPA.

The thematic analysis of the literature, coupled with a strong foundation of historical privacy references, yielded several themes. The themes highlight the convoluted topic of privacy and legislation and how privacy vanishes from users.

Themes in Privacy and Convenience

The thematic analysis identified four primary themes that capture the essence of the current dialogue on privacy and convenience:

Gaps in Law

Legislation, both foreign and domestic, based on the conception of privacy has been declared, sanctioned and preserved around the world. As discussed in this study, privacy has been a long discussion rich in ideas and changes riddled through history because of technological advancement. The analysis of the history of privacy details a severe contrast between privacy legislation within the U.S. and those of its counterparts. In the United States, the patchwork laws in limited states are not enough to protect its inhabitants and requires an all-encompassing, comprehensive law for regulation, the CCPA being the best example (Bonta 2023). The nation is able to develop a bill that mirrors GDPR but obeys the constitution, but the problem is that there is a lag in implementation.

Simply stated, the US puts privacy issues in the hands of the consumer, and GDPR puts privacy issues in the hands of the producer. A company exists to make money, and a comprehensive body of laws, such as GDPR/CCPA exists to ensure money is ethically made (General Data Protection Regulation, 2023).

The United States has been a strong supporter of privacy since the Universal Declaration of Human Rights (Amnesty International, n.d.). The gap in the US exists federally since there has been no law developed and statewide because only 5 states have worked on protecting their citizens (Bonta, 2023). With a precedent set in some states and the US showing support for privacy legislation around the world, there may be a likelihood that the nation will create federal legislation protecting digital privacy as an inviolable right.

Speed

The goal of technology is to improve people's quality of life by allowing them to complete a task much faster or automate it completely. Radio-frequency identification (RFID) is relatively secure but there are issues such as tracking that are possible due to traffic analysis that can affect location privacy (Abdulghani et al, 2022). RFID tags can be used in many devices and embedded in IoT devices such as credit card processors and hotel doors. Along with more technology and automation comes more data collection. David Eckhoff & Isabel Wagner (2017) stated, "The pervasiveness of applications and sensors leaves the individual citizen no choice but to become a digital part of future cities" (p. 1). The comment reflects the need for speed and convenience rather than security and encompasses all technology including mobile phones as being pervasive.

Within the last few years, strides have been made in technology in the interest of speed. Fingerprint scanners were added to laptops to escape typing a password, and Face ID was added to phones to bypass the need for security codes. Now, there is a service called Amazon One that trumps those. Amazon One is a service built for convenience that allows individuals to register their palms using a subcutaneous scan. The scan visualizes the underlying blood vessels to purchase goods at Amazon-owned companies such as Whole Foods, Panera and other Amazon stores (Dooley, 2023). Dooley (2023) believes in the convenience of palm scanning for purchasing goods to be a great idea in the name of convenience for the future. The issue is the private nature of all biometric data being freely given to corporations that are not medically required to handle any of the information responsibly.

Speed has two sides to it and they both lead to the same consequence. The first one is when a user chooses to ignore pervasive policies to use a product uninhibited (Obar & Oeldorf-Hirsch, 2020). The second is when a user recognizes pervasive technology and chooses to utilize it. In the interest of speed, individuals do not appear to realize what they give up obtaining it. Dooley (2023) expressed he was able to use iris scanner technology to get through airport security and facial recognition to board a flight. Inherently, the issues derive from questions of what is being done with the data and who can use it.

Perception of Security Awareness

The general public will often choose products based on public perception and not base their decisions on security quality. This notion can be observed when choosing a cellphone provider and even a car brand such as Tesla. People will buy a product because it is a dominant product in the market rather than the dominant option (Kim & Park, 2012). The same idea can extend to the security and privacy of a product. An example of choosing a product based on the dominant market would be a cell phone such as Apple's when other technology is available. Individuals also make inferences about security quality from convenience because convenience is observable, but security is not (Kim & Park, 2012). It is not always easy to determine the best option to use for a tool because personal research needs to be done. It is easy to make a choice based on majority rule but as Kim & Park (2012) mention, it is not always the best choice. Security awareness and decisions based on quality will benefit the consumer much more.

Public perception has much more to do with knowledge of a product. It also has to do with fear of the unknown. Through public outcries of national security by the government, fear is why people accept privacy invasions from the government (Schneier, 2015). The call for national security against terrorism, drugs and kidnapping eases Americans into giving up more rights for a sense of security.

While fear can play a massive part in public perception of privacy and security, the lack of knowledge plays another part entirely. A user may unknowingly participate in shady practices of data collection by buying a product and being forced into engaging with services. For example, when a consumer buys a Tesla, they buy the vehicle for many features such as self-driving, sentry mode to protect the car and to escape paying for gasoline. However, sentry mode can be turned on inside a person's garage and used to

spy on the owners of the vehicle. Tesla vehicles were found to have recorded intimate moments, nudity and a person being dragged against their will (Stecklow et al., 2023). When individuals buy their Tesla, they expect the camera features to be used to steer the car and train their algorithms so that they do not spy on them in their dwellings.

Much of the issues in awareness stem from EULAs and cookies not being read and understood by the enjoyer of the product. Obar & Oeldorf-Hirsch's (2020) study found that participants of the study viewed policies as a nuisance and ignored them for digital use rather than be inhibited by the means. Put clearly, individuals are skipping past the policies with information that explains what will be gathered from them so they can expedite being able to use the software.

Security awareness and public perception affect a user's ability to install a program, continue to use a program, and understand the circumstances surrounding the use of a program. Policies produced by companies are the first step to using a product, and people do not read them because the policies are lengthy (Good et al., 2005). However, Yerby & Vaughn (2022) highlight that companies deliberately create unreasonably long terms of service agreements or craft them to be intentionally vague to accomplish their goals. Yerby & Floyd (2018) argue that if organizations argue security awareness is vital and if policies are to be followed, they must be understandable or memorable. They go on to say that if the awareness is not meaningful, in this situation, a EULA, then it is essentially a ruse to protect the organization from legal action.

Services in Technology

Services in technology are prominent but many of those services violate privacy for convenience. For example, applications such as TikTok, YouTube, Google, and Amazon collect data and create unique user profiles daily. Companies reportedly surveil consumers while they are connected to the internet spying on their friends and family, browsing and purchasing histories as well as location and physical movements (Regulatory Update, 2022). Privacy is becoming a precious commodity that is not completely understood. Ozeran and the team of researchers stated, "Technology companies publicly devalue personal information to make it appear that we gain much more than we surrender" (Ozeran et al, 2021, p. 275). This point can be further proven when you pay attention to consumer behavior. Research suggests that people are willing to trade their email addresses for money or the chance to win a prize (Gerber et al, 2018). Companies seemingly participate in a form of digital entrapment by making the transaction seem appealing to a user to forfeit their digital rights.

One should be wary of using any free application, especially one such as TikTok. According to a case study about TikTok the downloading, creating and accessing of a TikTok account, users voluntarily allow the creator to collect data for the benefit of the company (Indrayani & Maharani, 2022). Unbeknownst to the user, to have the satisfaction of watching videos they may be surrendering more information than they were immediately willing to.

Discussion

The emerging themes paint a picture of society and the rush toward digital convenience without balancing and protecting the perceived inviolable right to privacy. Convenience itself is the improvement of quality of life, yet society demonstrates a lack of fundamental concern for their privacy. People will choose the easiest option for a service, as we see with self-driving cars, saved passwords on a web browser and face recognition software. Without a comprehensive, cohesive, and exhaustive statute similar to GDPR or CCPA for the entire United States, people will continue to relinquish their data at the cost of convenience. Legislation currently does not require an EULA or privacy policy within the US, but having the documents protects the company.

If a person does not understand the policies put in place but wishes to use the product regardless, we see they will continue to use the product at the cost of their privacy because of a lack of regulation. Therefore, a company can request anything or be as vague as possible with their policy, and in a court of law, they are always protected even through an overstep in data collection. Companies tracking friends and family and their physical movements are an example of the overstep because of no regulations for prevention.

Issues related to privacy based on the review of literature and results section of the study point out that legislation may play a big factor. Security awareness in terms of service and EULAs is too much going on, and consumers lack comprehension. Readable contracts in simple language are a possibility to prevent people from divulging personal information. The CCPA is a good step in the right direction in terms of ratified and backed legislation in the United States.

Issues exist when buying IoT devices as well. Buying a car such as a Tesla is now essentially buying an IoT device because it is electronic. It is unlikely that a user who buys a vehicle consents to privacy violations within their home, even if they consent to buying an electronic vehicle. When a person buys a car, they expect to drive it from point "A" to point "B" and do not have to read a detailed EULA to understand everything that is probable in owning one. The gap exists as long as there is no requirement to have clear, concise and comprehensive privacy policies for consumers to accept.

Technological advancements with no modern advancement of ratified law to match create a larger digital divide between convenience and privacy. The ubiquity of data collection technologies, from RFID to biometric scanning, presents a double-edged sword, enhancing user experiences while posing substantial privacy risks. The dichotomy that presents itself is an ever-increasing need for a truly comprehensive bill within the United States that governs people's right to inviolable digital rights.

Conclusion

Privacy itself can have an extreme amount of nuance due to the fluidity of the subject. Narrowing down privacy to convenience allows for an in-depth discussion and findings on the subject. Those findings curated the four overarching themes listed in the results section: laws, speed, public perception/security awareness and services. The themes discovered present challenges within the topic but many opportunities for improvement. The findings of this research accentuate the urgency for an all-encompassing and comprehensive privacy legislation that mirrors GDPR and is tailored to fit the United States and its constitution. Technology will continue to mature rapidly, and the safeguarding of US citizens' digital rights should match so convenience does not become a currency traded for the right to privacy.

Without clear and concise privacy policies users submit to arbitrary rules curated by companies who seek monetary gain by users not having coherent policies. Shifting to a new model of readable contracts sets a higher standard of security awareness and develops a privacy-conscious society. A privacy-centric and conscious society creates a harmonious existence between convenience and technology that is antithetical to today's existence.

The discourse surrounding privacy in the age of digital convenience is far from concluded. As this narrative review suggests, privacy is not dead, but it is at a critical juncture. The path forward demands a reevaluation of values, priorities, and the role of legislation in shaping a future where privacy is respected as an inalienable right, not a negotiable commodity.

References

Abdulghani, A. H., Nijdam, A. N., & Konstantas, D. (2022). Analysis on security and privacy guidelines: RFID-Based IoT applications. *IEEEAccess, 10,* 131528-131554. https://doi.org/10.1109/ACCESS.2022.3227449

Amnesty International. (n.d.). Universal declaration of human rights. https://www.amnesty.org/en/what-we-do/universal-declaration-of-human-rights/#:~:text=Work%20on%20the%20UDHR%20began,the%20USA%2C%20Lebanon%20and%20China

Ashley, C. K. (2020). Data of the dead: A proposal for protecting posthumous data privacy. *William and Mary Law Review, 62*(2), 649-682.

Aziz, A., & Telang, R. (2016). What is a digital cookie worth? *Social Science Research Network*. http://dx.doi.org/10.2139/ssrn.2757235

Bonta, R. (2023, May 10). California consumer privacy act (CCPA). *State of California Department of Justice.* https://oag.ca.gov/privacy/ccpa

Braun, V., & Clarke, V. (2006) Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77-101. https://doi.org/10.1191/1478088706qp063oa

Dooley, R. (2023, November 28). *Is amazon one the future of biometrics? Better business through behavioral science.* Forbes. https://www.forbes.com/sites/rogerdooley/2023/11/28/is-amazon-one-the-future-of-biometrics/?sh=6f745f1ad548

Eckhoff, D., & Wagner, I. (2017). Privacy in the smart city – applications, technologies, challenges, and solutions. *IEEE, 20*(1), https://doi.org/10.1109/COMST.2017.2748998

Ericson, D. J., Albert, S. W., Bernard, P. B., & Brown, E. (2022). End-User license agreements (EULAs): Investigating the impact of human-centered design on perceived usability, attitudes, and anticipated behavior. *Information Design Journal, 26*(3). 190-208. https://doi.org/10.1075/idj.20018.eri

General Data Protection Regulation. (2023). Right to erasure ('right to be forgotten'). GDPR.eu. https://gdpr.eu/article-17-right-to-be-forgotten/

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Science Direct,* 77, 226-261. https://doi.org/10.1016/j.cose.2018.04.002

Gilman, E. M., (2020). Five privacy principles (from the GDPR) the United States should adopt to advance economic justice. *Arizona State Law Journal, 52*(2), 368-444.

Good, N., Dhamija, R., Grossklags, J., Thaw, D., Aronowitz, S., Mulligan, D., & Konstan, J. (2005). Stopping spyware at the gate: A user study of privacy, notice and spyware. *ACM Digital Library.* https://doi.org/10.1145/1073001.1073006

Hoofnagle, J. C., van der Sloot, B., & Borgesius, Z. F. (2019) The European union general data protection protection regulation: what it is and what it means. *Information and Communications Technology Law, 28*(1), 65-98. https://doi.org/10.1080/13600834.2019.1573501

Indrayani, I., & Maharani, T. (2022). The united state's national security protection from cyber crime threats a case study of tik tok banning submission by the president Donald Trump in 2020. *Journal of Social Political Sciences, 3*(3). 268-280 https://doi.org/10.52166/jsps.v3i3.122

Jones, K. (2004). Mission drift in qualitative research, or moving toward a systematic review of qualitative studies, moving back to a more systematic narrative review. *Qualitative Report*, *9*(1), 95–112.

Kim, C. B., & Park, W. Y. (2012). Security veresus convenience? An experimental study of user misperceptions of wireless internet service quality. *Decision Support Systems, 53*(1), 1-11. https://doi.org/10.1016/j.dss.2011.08.006

Krupp, F. A. (2022). Privacy is not dead: Expressively using law to push back against corporate deregulators and meaningfully protect data privacy rights. *Georgia Law Review, 57*(2), 874-918.

Obar, J. & 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

Ozeran, L., Solomonides. A., & Schrieber. R. (2021). Privacy versus convenience: A historical perspective, analysis of risks, and an informatics call to action. *NIH, 12*(2), 274-284. https://doi.org/10.1055/s-0041-1727197

Regulatory update: Attorney general Mark Brnovich achieves historic $85 million settlement with google (2022, October). *Journal of Internet Law, 26*(3), 3-10. https://eds.p.ebscohost.com/eds/detail/detail?vid=0&sid=c5a8e26a-60e0-4800-91d1-42ad717fa27a%40redis&bdata=JkF1dGhUeXBlPWlwLHNoaWImc2l0ZT1lZHMtbGl2ZSZzY29wZT1zaXRl#AN=160224222&db=bth

Schneier, B. (2015). Fear and convenience. In M. Rotenberg, J. Horwitz, & J. Scott (Eds.), Privacy in the modern age: The search for solutions (pp. 200-203). The New Press.

Stecklow, S., Cunningham, W., & Jin, H. (2023, April 6). *Tesla workers shared sensitive images recorded by customer cars.* Reuters. https://www.reuters.com/technology/tesla-workers-shared-sensitive-images-recorded-by-customer-cars-2023-04-06/

Warren, D. S., & Brandeis, D. L. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193-220. https://doi.org/10.2307/1321160

Westin, F. A. (1966). Science, privacy, and freedom: Issues and proposals for the 1970's. Part II: Balancing the conflicting demands of privacy, disclosure and surveillance. *Columbia Law Review, 66*(7), 1205-1253. https://doi.org/10.2307/1321160

Yerby, J., & Floyd, K. (2018). Faculty and staff information security awareness and behaviors. *Journal of The Colloquium for Information Systems Security Education, 6*(1) https://cisse.info/journal/index.php/cisse/article/view/90

Yerby, J. & Vaughn, I. (2022). Deliberately confusing language in terms of service and privacy policy agreements. *Issues in Information Systems, 23*(2). https://doi.org/10.48009/2_iis_2022_112