SAIS 2023 Proceedings | Southern (SAIS)

7-1-2023

Identifying tomorrow’s Smart City Privacy Challenges: A Review of Literature

John Wilkerson

James Smith

IDENTIFYING TOMORROW'S SMART CITY PRIVACY CHALLENGES: A REVIEW OF LITERATURE

John Wilkerson
Augusta University
Jowilkerson@augusta.edu

James N. Smith
Augusta University
Jasmith8@augusta.edu

ABSTRACT

The right to privacy's foundation is supported by four pillars; the right to private facts, the right to prohibit others from using one's likeness, the right to challenge defamation claims, and the right to unreasonable personal intrusion. Tomorrow's "high-tech" Smart City is characterized by countless digital consumer privacy and information security triggers which challenge Americans' right to protect their personal identifiable information. The pressing privacy question is, are consumers aware of the privacy implications when navigating across Smart Cities? This literature review implements a mixed-method research strategy. First, this paper examines the roles of the theories of information flow, social contracts, and being left alone in digital consumer identity theft. Second, this research explores federal and state government agencies privacy policies to understand potential Smart City ecosystem privacy gaps. This literature review reveals predictable and unpredictable trends and patterns which could contribute to digital consumer privacy flaws and cyber complaints.

Keywords

Privacy Policy, Privacy Gaps, Smart City, Digital Consumer

INTRODUCTION

Protecting digital consumer privacy and personal identifiable information (PII) has been a complex high-tech Smart City topic for years. The US Federal Bureau of Investigation 2021 Internet Crime Report asserts that more than 2.75 million consumers filed cyber-crime complaints, which resulted in $18.7 billion in losses from 2017-2021 (Abbate, 2022). This FBI report points out that 427,430 cyber violations such as identity theft, personal data breach, and phishing directly targeted digital consumers in 2021, a 31% year-over-year increase (Abbate, 2022). Clearly, protecting digital consumers PII is a privacy topic that is an emerging problem which impacts federal, state, and local smart cities.

Digital consumer privacy research has expanded since 2017. Countless information security studies scholars have addressed technical problems, user compliance, and security education training and awareness (SETA). Thus, a comprehensive literature review which balances theory and contemporary data is required to tackle consumer privacy and enterprise interest is appropriate. This literature review seeks to identify these sometimes-hidden privacy issues. This paper has analyzed 100 privacy policies published in 2018. These policies were analyzed and sorted by important inclusive and exclusive criteria. This mixed methods research investigated three privacy theories which identities privacy and monetary tension across high-tech Smart Cities. Theory one, Wua, Chiub, Chena (2020)'s theory of information flow creates an effective information distribution to communicate key messaging across tomorrow's smart cities. The theory of information flow is an emotional response to online marketing hence a key segment of this paper's literature review. Theory two, Martin (2016)'s theory of social contract, creates a healthcare and federal government PII ethical dilemma. The theory of social contract asserts that agencies and enterprises are ethically bound to protect segments of digital consumers PII, with few limitations. Theory three, Acquisti and Grossklags (2005) theory of "being left alone" points out that numerous Smart City actors undervalue digital consumer privacy. Privacy scholars Milne and Culnan (2004), Cho, Lee, and Chung (2010), Casado-Aranda, Sánchez-Fernández, and Montoro-Ríos (2018), and Crepax, Muntés-Mulero, Martinez, and Ruiz (2022) support the theory of "being left alone" argument and emphasize digital consumers must understand online privacy risks. This paper's privacy theories reveal a digital consumer privacy gap and a need for more thorough research. Therefore, this literature review is laser-focused on addressing one niche privacy compliance research question, are digital consumers aware of the privacy implications when navigating across Smart Cities?

Legal Characteristics

Maxeiner (2018) suggests that the US constitution provides the foundation for the American legal system, American government, and international stability. Vile (2021) describes seven articles and twenty-seven amendments that make up the US constitution. Federal and state governments create laws and operate numerous court systems. Grama (2020) asserts that certain codes, statutes, and civil torts are based on court decisions or prior precedence. The 4th amendment of the US constitution does not allow unreasonable search and seizures without probable cause for a lawful warrant. The US Privacy Act of 1974, 5 U.S.C. § 552a enforces limits on the amount of PII an agency or enterprise can collect. The Cable Communications Policy Act of 1984 oversees the PII that cable enterprises collect. The Electronic Communications Privacy Act of 2000 regulates email and other electronic communications. Collectively these federal laws and numerous state and local laws are designed to protect digital consumer privacy interests.

Nevertheless, Swire (1997) asserts that internet privacy practices to protect digital consumers are based on self-regulation guiding principles. This volunteer compliance principle opens the door to agency and enterprise 4th amendment rights violations. Given the recent court's precedent and tradition decision, Smart City policymakers have a dilemma, how to protect digital consumers' PII.

METHODOLOGY

A literature review provides the foundation for a research study, illuminating what is known about a topic so that gaps in knowledge are revealed. This study reveals privacy policy dilemmas that present a consistent trend across this paper's diverse study group. A literature review is a comprehensive process to identify, investigate, and synthesize scholarly digital consumer literature authored by the scholarly community. This paper followed a four-step sequential interview review process. The first step in this paper's literature search process was an exploratory search. An exploratory search begins with identifying initial keywords, databases, and sources. Researchers seeking to follow this step can use the keywords to get started. Qualitative researchers Schlagenhaufer and Amberg (2015) described the next step, descriptive literature review. This step identifies the potential gaps in the literature, classifies material, and creates linkages across the literature (Lyman-Hager, 2000). The third step in the literature review process is explanatory; privacy researchers Schaewitz, Winter, and Krämer (2021) characterized "explanatory" as analyzing the data, refining research questions, and seeking to understand patterns and trends. The last step in this study's literature review process is titled predictive. Van Egmond et al. (2021) imply that new privacy theories or frameworks are achievable after analyzing the literature (qualitative) and data (quantitative).

This paper's privacy sources ranged from peer review articles, government privacy policies, and other privacy policies. This literature review followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) evidence-based data collection strategy by describing all databases and sources. Nearly 50 percent of peer-reviewed papers were published from 1968-2016. More than 50 percent of peer-reviewed papers were published from 2017-2022. All federal and state government privacy policies were published in 2018.

Source Type	6 Years and Older	5 Years and Younger	Total
Journal Articles	14	14	28
Dissertation / Master’s Thesis	0	3	3
Conference Proceedings	0	2	2
Government Privacy Policies	0	30	30
Other Sources	0	2	2
Total	14	51	65

Table 1. Literature Review Sources

The paper utilized journal articles, dissertations, thesis, conference proceedings, and privacy policies written in English. After the explanatory phase, this literature review narrowed its research question and developed important patterns. Once patterns were formed, this research developed literature inclusion and exclusion criteria. The purpose of clustering the research criteria during the predictive phase is to help develop a rigorous privacy research framework. This paper’s inclusion and exclusion criteria include:

Inclusion Criteria	Exclusion Criteria
English-only privacy policies	Policies that do not address digital consumer social media compliance
Policies from federal law enforcement agencies	Policies that do not address internet platform technical compliance
Policies from state law enforcement agencies	Policies that do not address internet service provider compliance
Policies from federal healthcare agencies	Policies that do not address SETA
Policies from state healthcare agencies	All city government privacy policies are excluded
Policies published in 2018 only	
Policies do not have download restrictions.	

Table 2. Inclusion Exclusion Criteria

According to Creswell (2014), a literature review map is an effective investigation tool for reviewing and analyzing literature. Three research themes characterize this paper's literature review map; Smart City privacy policy theories, federal government privacy policies, and state government privacy policies related to this research question. As this study's literature review developed, the association between the literature and the research question also evolved.

The output of this paper's sequential literature review process and literature review map is the foundation for this study. The output includes a rigorous privacy research framework, research themes, and knowledge gaps focused on protecting digital consumer privacy in tomorrow's smart cities. Key components included three theories, federal and state government privacy policies. Examining the Smart City privacy policy ecosystem provides a compelling framework to address user compliance and policy violations.

Findings

The final phase of this literature review is a qualitative analysis. Findings from the literature review will answer the key research question, "are digital consumers aware of the privacy implications when navigating across Smart Cities?". This literature review study group findings primarily included nominal data. Perreault and Leigh (1989) suggest that nominal data reduces research risk because categorical data is closed-ended and is considered more reliable than other types of data. This digital consumer privacy literature review has nine independent variables selected from the leading United States law enforcement agency tasked with protecting digital consumer privacy. This study validated each independent variable with two additional federal agencies responsible for protecting digital consumer privacy. Next, this literature review increased research rigor by analyzing state agencies. This research protects study group participant confidentiality by coding and tabulating findings across each independent variable. Three state agencies were included in this paper's study group.

Relevant Theories

Theory Of Information Flow

Birnhack (2011), Ampong, Mensah, Adu, Addae, Omoregie, and Ofori (2018), and Wua, Chiub, and Chena (2020) argue that the internet is an open environment to exchange ideas, conduct business operations, and conduct ecommerce activities. These authors imply that online platforms are more valuable than harmful to today's users. The theory of information flow advocates that users' internet video, imagines, and posts are privacy violations. Malik, Hiekkanen, Dhir, and Nieminen (2016) point out that 1.8 billion videos are posted on the five leading social media sites daily. The online environment is an identity fraudsters moneymaker. Government agencies are bound to educate digital consumers and publish privacy policies. For example, Federal Agency, FedL1 is 100% committed to protecting digital consumers privacy. However, digital consumers agree to FedL1 data collection privacy policy. The following data is automatically shared when landing on this agency's website; Consumer's domain name, browser details, operating system, Internet Protocol (IP) address, date and time, link origin, and on-site activity. In contrast, to the federal government example, similar to FedL1, Fp1 is a private online enterprise 100% devoted to protecting digital consumers privacy. Yet, website visitors grant Fp1 permission to collect the following digital consumer data; Consumer name, address, email address, telephone number, credit card number, and photograph. The internet theory of information flow has a tremendous business, social, and economic potential. However, are digital consumers aware of the privacy implications when navigating across Smart Cities?

Theory of Social Contracts

Social Contract Theorists Morris (1999) argue that a social contract is mislabeled. He suggests that a social contract is an agreement aligned with self-interest. Martin (2016) implies that online platforms are ethically bound to protect digital consumer privacy. Liaropoulos (2020) points out that in a period of billions of online transactions per day, privacy violations are likely to occur. For example, all Federal Agencies (study group) comply with email, marketing, and cookies privacy requirements.

Nevertheless, during this paper's data collection phase, StH2 fully commit to sharing digital consumer data. According to StH2 privacy policy, the state utilizes log files or cookies collect the following digital consumer data; Consumer name, address, email address, driver's license number, telephone number, credit card number, social security number, username, and password. In comparison, the state (StH2) privacy violation, FedH1 and FedL2 are federal agencies fully committed to not disclosing privacy information, including; consumer name, profile, email address, username, and password. It appears this study group’s federal government agencies are fully committed to the theory of social contracts. Nevertheless, are digital consumers aware of the privacy implications when navigating across Smart Cities?

Theory of Being Left Alone

Culnan and Armstrong (1999), Chellappa and Sin (2005), and Belanger and Crossler (2011) argue that individuals (digital consumers) may limit their online primacy risk by digesting online disclosures and evaluating benefits and risks. Punj (2018) asserts that the theory of being left alone must meet conditions. One, the digital consumer must understand the value of the information. For instance, is a digital consumer's online privacy more important than posting new baby pictures? Two, the volume of information one must digest. Case in point, where are privacy and the scholarly tradeoff for elite high school students? Three, digital consumers desire to control their personal information. For example, are high schools likely to clean their cookies or pixels after closing their browser hourly, weekly, or monthly? The theory of being left alone has tangible theoretical and empirical impalements because 50% of this literature review study group did not comply with federal Children’s Online Privacy Protection Act (COPPA) standards. StL3's privacy policy points out that the state does not purposely collect data from anyone under the age of 18 years old. It appears that all federal study group participants did protect children's youth interests. Nevertheless, are young digital consumers fully aware of the privacy implications when navigating across federal and state government's internet online platforms?

ANALYSIS

When applied to this literature review, theories demonstrate not surprising online privacy trends and patterns when considering the $18.7 billion in digital consumer losses from 2017-2021. For example, Fried (1968) describes privacy as granting access to others by choice. The theory of information flow asserts that digital consumers who post videos, imagines, blog posts are giving up their right to privacy. 100% of this paper's federal and state government privacy policies voluntarily complied with the US Privacy Act and other relevant laws. This privacy policy gap is one contributing factor to the 2.75 digital consumer privacy complaints (identity theft, personal data breach, and phishing) in 2021.

Miller (2010) describes digital consumers prefer to engage in an online platform that binds the digital assets to ethically protect user's privacy. The Theory of Social Contracts points out that billions of digital consumer privacy violations daily do not meet a lawful contract standard. Nevertheless, 100% of this literature review's federal and state government privacy policies voluntarily complied with the US Privacy Act and other relevant laws. In comparison, 90% of the study group states complied with state government privacy policies. Lastly, Berlin (2002) argues that it is a digital consumer's fundamental right to navigate across the internet without privacy concerns. The theory of being left alone adult and child digital consumers may limit their risks by evaluating privacy policies. 100% of this literature review's federal state government privacy policies agreed to meet the US Privacy Act and other relevant laws. In contrast, 66% of the study group states complied with state government privacy policies. In comparison, 50% of this literature review's for-profit group met the federal privacy policy standard. Given the online threat, this significant privacy policy disappointment could negatively influence privacy for countless years for adults and children. The theory of information flow, theory of social contracts, and theory of being left alone reveal interesting patterns which apply to Smart City policymakers when applied to this literature private policy research. Not surprisingly, federal governments comply with federal privacy laws. Yet, unpredictably, some state governments did not comply with privacy policy laws during this study. Prior to this study, it was expected that all federal and state agencies would comply with privacy standards. One unexpected shock from this research is that some state agencies may have limited regard for children privacy.

CONCLUSION

The study explores one important research question are digital consumers aware of the privacy implications when navigating across Smart Cities? This research suggests that consumers who openly post videos, post blogs, and images likely consider online platforms more beneficial than harmful. The paper asserts that billions of digital consumer violations occur daily with limited consumer pushback. This literature review also points out that parents or guardians do not fully adopt children's privacy protections. Nevertheless, hundreds of thousands of digital consumers are identity theft, personal data breach, and phishing victims. These victims continue to engage various Smart City platforms. On the other hand, federal privacy laws should be followed. This study reveals that 100% of this paper's federal study group complied with privacy policies. Conversely, this research describes that some state governments do not abide by federal privacy standards. This paper concludes that digital consumers are not fully aware of Smart City's privacy implications.

In the future, privacy researchers may consider expanding the study group and addressing two questions. One, are federal and state privacy policies written for the typical digital consumer? Two, is there a direct correlation between limited children's privacy policy adherence and federal or state interest? In order to comply with Institutional Review Board (IRB) subject privacy and confidentiality requirements, this study will not cite specific privacy policies named in this paper.

References

1. Abbate, P. (2021). The 2021 Internet Crime Report. Internet Crime Complaint Center, US Federal Bureau of Investigation. Retrieved from https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf?aff_id=07896725
2. Acquisti, A., & Grossklags, J. (2005). Privacy and Rationality in Individual Decision Making. IEEE Security & Privacy, 3(1), 26-33.
3. Amos, R., Acar, G., Lucherini, E., Kshirsagar, M., Narayanan, A., & Mayer, J. (2021). Privacy Policies Over Time: Curation and Analysis of a Million-Document Dataset. In Proceedings of the Web Conference 2021 (pp. 2165-2176).
4. Ampong, G. O., Mensah, A., Adu, A., Addae, J., Omoregie, O., & Ofori, K. (2018). Examining Self-Disclosure on Social Networking Sites: A Flow Theory and Privacy Perspective. Behavioral Sciences, 8(6), 58.
5. Belanger, F., and Crossler, R. (2011) Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. Journal of Management Information Systems. Q 35(4),1017–1042.
6. Berlin, I. 2002. "Two Concepts of Liberty" (1958), in Liberty, ed. Henry Hardy, 166–217. New York: Oxford University Press.
7. Birnhack, M. D. (2011). A Quest for a Theory of Privacy: Context and Control. Review of Privacy in Context: Technology, Policy, and The Integrity of Social Life. Jurimetrics, 51(4), 447–479.
8. Casado-Aranda, L. A., Sánchez-Fernández, J., & Montoro-Ríos, F. J. (2018). How Consumers Process Online Privacy, Financial, and Performance Risks: An MRI Study. Cyberpsychology, Behavior, and Social Networking, 21(9), 556-562.
9. Chellappa R., & Sin R. (2005) Personalization Versus Privacy: An Empirical Examination of The Online Consumer's Dilemma. Information Technology Management 6(2), 181–202.
10. Cho, H., Lee, J. S., & Chung, S. (2010). Optimistic Bias About Online Privacy Risks: Testing the Moderating Effects of Perceived Controllability and Prior Experience. Computers in Human Behavior, 26(5), 987-995.
11. Crepax, T., Muntés-Mulero, V., Martinez, J., & Ruiz, A. (2022). Information Technologies Exposing Children to Privacy Risks: Domains and Children-Specific Technical Controls. Computer Standards & Interfaces, 82, 103624.
12. Creswell, J. W. (2014). Research Design: Qualitative, Quantitative, and Mixed Approach Methods (4th ed.). Thousand Oaks, CA: Sage.
13. Culnan M. and Armstrong, P.K. (1999) Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. Organizational Science 10(1), 104–115.
14. Fried, C. 1968. "Privacy [A Moral Analysis]," in Philosophical Dimensions of Privacy: An Anthology, 203–23. Cambridge: Cambridge University Press.
15. Grama, J. L. (2020). Legal and Privacy Issues in Information Security. (3rd Edition). Burlington, MA. Jones & Bartlett Learning.
16. Lyman-Hager, M. A. (2000). Bridging the Language-Literature Gap: Introducing Literature Electronically to the Undergraduate Language Student. CALICO Journal, 17(3), 431-452.
17. Malik, A., Hiekkanen, K., Dhir, A., Nieminen, M. (2016). Impact of Privacy, Trust, and User Activity on Intentions to Share Facebook Photos. Information Ethics Society. 364–382.

18. Miller, D. (2010). "Why Immigration Controls Are Not Coercive: A Reply to Arash Alizadeh," Political Theory, 38(1): 111–0.
19. Milne, G., & Culnan, M. (2004). Strategies for Reducing Online Privacy Risks: Why Consumers Read (Or Don't Read) Online Privacy Notices. Journal of interactive marketing, 18(3), 15-29.
20. Morris., C. W. (1999). The Social Contract Theorists: Critical Essays on Hobbes, Locke, and Rousseau. Rowman & Littlefield Publishers.
21. Perreault Jr, W. D., & Leigh, L. E. (1989). Reliability of Nominal Data Based on Qualitative Judgments. Journal of Marketing Research, 26(2), 135-148.
22. Peslak, A. R. (2005). Internet Privacy Policies: A Review and Survey of the Fortune 50. Information Resources Management Journal (IRMJ), 18(1), 29-41.
23. Punj, G. N. (2018). Understanding Individuals' Intentions to Limit Online Personal Information Disclosures to Protect Their Privacy: Implications for Organizations and Public Policy. Information Technology and Management Journal.
24. Schaewitz, L., Winter, S., & Kramer, N. (2021). The Influence of Privacy Control Options on The Evaluation and User Acceptance of Mobile Applications for Volunteers in Crisis Situations. Behaviour & Information Technology, 40(8), 759–775.
25. Schlagenhaufer, C. & Amberg, M. (2015). A Descriptive Literature Review and Classification Framework for Gamification in Information Systems. ECIS 2015 Completed Research Papers. Paper 161. doi:10.18151/7217466
26. Swire, P. (1997). Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information, in Privacy and Self-Regulation in the Information Age by the US Department of Commerce. US Department of Commerce.
27. Wu, L., Chiu, M. L., & Chen, K. W. (2020). Defining the Determinants of Online Impulse Buying Through a Shopping Process of Integrating Perceived Risk, Expectation- Confirmation Model, and Flow Theory Issues. International Journal of Information Management, 52, 102099.
28. Van Egmond, M., Spini, G., Van der Galien, O., IJpma, A., Veugen, T., Kraaij, W., & Kooij-Janic, M. (2021). Privacy-Preserving Dataset Combination and Lasso Regression for Healthcare Predictions. BMC Medical Informatics & Decision Making, 21 (1). 1–16.
29. Vile, J. (2021). A Companion to The United States Constitution and Its Amendments. Santa Barbara, CA. Praeger.