2023

# Investigating Protected Health Information Privacy: Smart City Policymaker Challenges

John Wilkerson

Marcia Dailey

Paul Brown

# Investigating Protected Health Information Privacy: Smart City Policymaker Challenges

**John Wilkerson**
Augusta University
jowilkerson@augusta.edu

**Marcia Dailey**
Clark Atlanta University
mdaley@cau.edu

**Paul Brown**
Clark Atlanta University
pbrown1@cau.edu

## ABSTRACT

Smart Cities are characterized as urban information and communication technology hubs focused on renovating community healthcare ecosystems. Expanded smartphones, tablets, and internet of things (IoT) use have increased fears about digital healthcare consumers privacy. These protected healthcare information privacy concerns create a new sense of urgency for Information Security researchers to investigate complex digital healthcare consumer behaviors. This paper brings Smart City policymaker information security awareness by exploring the current state of protected healthcare information privacy through institutional information security privacy policies. This paper's theoretical contributions asserts that scholars should focus on digital healthcare consumers behaviors in Smart Cities. This foundational research study reveals contradictions and interesting privacy considerations for federal, state, and city government policymakers.

### Keywords

Protected Health Information, Personal Healthcare Information, Data Privacy Gaps, Privacy and Security, Smart City Policy

## INTRODUCTION

Agencies within and across institutions share healthcare information to best serve patients. In doing so, they must balance the security and privacy concerns of the patients and the advantages of accessibility. Preserving digital consumers' protected healthcare information (PHI) privacy across tomorrow's Smart City (SC) is likely a complicated challenge for the Information Security, Legal, and Risk Management domains. Bakıcı, Almirall, and Wareham (2013) characterizes Smart Cities as urban information and communication technologies (ICT) centers focused on modernizing the economy, environment, and healthcare domains. According to the Federal Trade Commission (FTC), from 1996-2019, 98 hospitals, prescription drug manufacturers, and retail pharmacies were issued punitive discipline for violating PHI privacy regulatory mandates (FTC, 2023). The FTC data indicates that 52 of 98 regulatory investigations imply healthcare privacy gaps throughout physician networks, individual medical and dental clinics, and various healthcare advocacy associations. Safeguarding digital health consumers' PHI is a crucial agenda item for SC policymakers and the US healthcare ecosystem.

The PHI and Information Security (InfoSec) body of knowledge has grown since the 1990s. In contrast, the scholarly community considers SC InfoSec literature an emerging topic. InfoSec and SC researchers are making tremendous progress by addressing training, awareness, and new technology research domains. However, an inclusive research study that balances existing theory and modern data is required, and this study is very timely, to address digital consumer PHI privacy. This research reveals critical digital healthcare consumers privacy issues that SC Policymakers must consider. This qualitative study investigated privacy theories and asks the question: Are digital healthcare consumers aware of the privacy implications when navigating the Smart City healthcare digital ecosystem?

## SMART CITY LEGAL CHARACTERISTICS

Decades ago, Berry (1964) inferred that the urban social science body of knowledge had room to grow. Kitchin (2014) and Adler and Florida (2021) suggest smart cities use ICT to boost efficiency and enhance many aspects of digital citizen lives. However, smart cities are not cure-all economic, environmental, and healthcare equity solutions without risks. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191 limits PHI electronic, written, and oral demographic data collection and use. However, the risks for governments are unintentional PHI data collection and dissemination while implementing digital healthcare policies for the public good.

In contrast to federal law, Swire (1997) asserts that internet privacy practices to protect digital healthcare consumers are based on implied and self-regulation guiding principles. This volunteer compliance principle opens the door to 4th amendment rights' violations for government agencies. Given the recent court's precedent and definitive decision, SC policymakers have a dilemma, how to protect digital consumers' PHI.

## METHODOLOGY

This paper explored the InfoSec body of knowledge from conferences and prevalent databases from 1992-2022. More than 50 journal articles from AIS library, Google Scholar, Information Systems Research, Management Science, and MIS Quarterly. Initial research terms include "protected health information", "digital healthcare", "PHI privacy", and "privacy policy". Papers and reference sections were reviewed. A new search terms were included "Smart City privacy", "digital consumer healthcare", "human-centered behavior".

Next, this paper reviewed several law enforcement and healthcare agencies focused for developing PHI and standards and guidelines. Privacy policy criteria was developed to evaluate other federal and state agencies. Each federal and state government privacy policy was published from 2018-2022. Each study and policy were reviewed and accepted or rejected. This paper's inclusion and exclusion criteria includes the following:

| Inclusion Criteria | Exclusion Criteria |
|---|---|
| English-only privacy policies | Policies that do not address digital healthcare 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 – 2022 | All for-profit privacy policies are excluded |
| Policies do not have download restrictions | |

**Table 1: Inclusion – Exclusion Criteria**

## RELEVANT THEORIES

Theory of Social Contract

Many privacies scholars Ritchie (1891) and Donaldson and Dunfee (1994), argue that the foundation for social contracts is built on normalizing ethical behavior. Donaldson and Dunfee (1994) further imply that 21st-century managers must balance ethics and business performance. In contrast, Netanel (2000) suggests that social contracts demonstrate that digital health consumers consent to PHI policies; however, federal privacy policies must be enforced.

Nevertheless, one healthcare and law enforcement agency's log files or cookies privacy policy stood out during this paper's data collection phase. One state tested social contract theory by collecting digital healthcare consumers' names, email addresses, driver's license numbers, social security numbers, usernames, and passwords. In comparison, other study group members complied with HIPAA privacy regulatory requirements. This study gives the impression that federal agencies are fully committed to the theory of social contracts and protecting digital

consumers' healthcare privacy. However, are our digital consumers aware of the privacy implications when navigating across Smart Cities?

Theory of Information Flow

Birnhack (2011) and Wua et al., (2020) argue that the internet is an open environment to exchange ideas, conduct

business operations, and conduct e-commerce activities. These authors infer that online platforms (healthcare apps) are more valuable than harmful to today's users. The theory of information flow advocates that users' internet video images and posts are privacy violations Milne and Culnan 2004. Federal and state government privacy policies are duty-bound to protect digital healthcare consumers. For example, each federal study group participant's privacy policies are 100% committed to protecting digital healthcare consumers' privacy. Nevertheless, digital healthcare consumers must agree to data collection policies. When a digital healthcare consumer lands on a study group online platform, the privacy policy requires the party to provide the consumer's domain name, browser details, operating system, internet protocol (IP) address, and origin.

In contrast, each state agency in this study group collects similar online data; however, some state agencies appear to collect some forms of children's PHI. For instance, parties (child ren) who land on specific state online platforms must agree to share names, addresses, email addresses, telephone numbers, and photographs. This research suggests that federal government agencies' privacy policies intend to meet HIPAA privacy standards. Nevertheless, are digital consumers aware of the privacy implications of navigating Smart Cities?

Theory of Being Left Alone

Laufer and Wolfe (1977), Culnan and Armstrong (1999), Netanel (2000), and Belanger and Crossler (2011) argue that individual (digital healthcare consumers) consent to being left alone when surfing across the Smart City healthcare ecosystem. Punj (2018) asserts that the theory of being left alone must meet three tests. First, the digital healthcare consumer must understand the value of the information. For instance, is a digital healthcare consumer's online privacy more important than posting new baby pictures which may expose a healthcare condition? Two, the volume of information not be harmful. Case in point, is it acceptable to implement COVID-19 booster immunization status on social media? Three, digital healthcare consumers desire to control one's personal information. Is it appropriate for school administrators to review students' search history in order to analyze sexual orientation?

The theory of being left alone has tangible theoretical and empirical significance because one state did not fully comply with federal (HIPAA) privacy requirements. For example, one state agency privacy policy (during this study period) asserts that the state does not purposely collect data from anyone under the age of 18 years old. A federal agency's s privacy policy for children indicates that children under 13 are not allowed on the platform without parental consent. Given the large children's homeless population and limited online controls, this federal agency policy may have a limited impact. This paper argues that federal and state agencies that balance the theory of being left alone with HIPAA compliance. This research implies that federal and state agencies intend to comply with (HIPAA) privacy values; however, some gaps may exist. The key question, are digital consumers aware of the privacy implications when navigating across Smart Cities? Agencies and enterprises which follow the digital healthcare consumer's the being left alone theory could have privacy policy gaps, hence a gap in the InfoSec body of knowledge. Smart City Policymakers, InfoSec, and risk managers must balance human-centered privacy and HIPAA requirements in the near future.

## ANALYSIS

Steinfeld (2016) assert that online digital consumers do not read privacy policies or contracts. This research study theories follow the premise; Smart City digital healthcare consumers may be not likely aware of PHI privacy policy implications when circumnavigating across Smart Governments. Case in point, Cava and Mayer (2006) and Ast (2019) infer that ethical and cultural norms have changed. Consequently, one may suggest that popular Olympic athletes who share medical test results are normalizing PHI disclosure for the ordinary fitness enthusiast.

Fried (1968) describes privacy as granting access to others by choice. This study suggests that the theory of

information flow does not support PHI privacy. For instance, Ross, Todd, and Saedi (2015) argue that some healthcare delivery organizations utilize cosmetic dermatology patient software as appealing visual marketing tools to entice digital healthcare consumers. Prospective patients that download these projected visual images do not adhere to the theory of information flow.

Berlin (2002) suggests that internet users have a right to privacy when surfing the internet. This study asserts that digital healthcare consumers who follow the theory of being left alone may be engaging in risky online behaviors. For example, 100% of this study's privacy policies meet US Privacy Act and other relevant laws. In contrast, 40% of the study group privacy policies failed to meet digital healthcare consumers' privacy policies. Given the online PHI threat, this immense privacy policy disappointment could negatively influence adults' and children's privacy for countless years.

This paper's findings reveal interesting patterns which apply to Smart City government policymakers. Findings from the study reveal, not surprisingly, that federal governments do comply with federal privacy laws. However, what was unexpected was the lack of compliance of some state governments with privacy policy law. Before this study, for-profit enterprises were expected to not comply with privacy standards. One unpredicted disappointment from this research is that some state agencies may not have complied with PHI privacy policies during this study period.

## CONCLUSION

This research study examines one crucial question, are digital healthcare consumers aware of the privacy implications when navigating across the Smart City healthcare digital ecosystem? This research suggests that digital healthcare consumers' willingness to post cosmetic, healthcare, fitness training content voluntarily surrender their right to privacy. Still the public and private ecosystem must follow HIPPA privacy mandates. This digital consumer and legal privacy challenge is low hanging fruit for future InfoSec and SC scholars.

This intent for this paper is to construct a foundation for deeper Social Determinants of Health, for-profit human-centered healthcare system, and children privacy policies gaps. 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. and Grossklags, J. (2005). Privacy and Rationality in Individual Decision Making. *IEEE Security & Privacy*, 3(1), 26-33.
3. Adler, P. and Florida, R. (2021). The Rise of Urban Tech: How Innovations For Cities Come From Cities. *Regional Studies Association*, 55(10-11), 1787-1800.
4. Bakıcı, T., Almirall, E., and Wareham, J. (2013). A Smart City Initiative: The Case of Barcelona. *Journal of the Knowledge Economy*, 4, 135-148.
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. Berry, B. (1964). Cities as Systems Within Systems of Cities. Papers in Regional Science, 13(1), 147-163.
8. Birnhack, M. (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.
9. Casado-Aranda, L. Sánchez-Fernández, J. and Montoro-Ríos, F. (2018). How Consumers Process Online Privacy, Financial, and Performance Risks: An MRI Study. *Cyberpsychology, Behavior, and Social Networking*, 21(9), 556-562.
10. Cava, A. and Mayer, D. (2007). Integrative Social Contract Theory and Urban Prosperity Initiatives. *Journal of Business Ethics*, 72, 263-278.

11. Chellappa R. and Sin R. (2005). Personalization Versus Privacy: An Empirical Examination of The Online Consumer's Dilemma. *Information Technology Management*, 6(2), 181–202.
12. Cho, H., Lee, J. and 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.
13. Crepax, T., Muntés-Mulero, V., Martinez, J. and Ruiz, A. (2022). Information Technologies Exposing Children to Privacy Risks: Domains and Children-Specific Technical Controls. *Computer Standards & Interfaces*, 82, 103624.
14. Creswell, J. (2014). Research Design: Qualitative, Quantitative, and Mixed Approach Methods (4th ed.). Thousand Oaks, CA: Sage.
15. Culnan M. and Armstrong, P.K. (1999) Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organizational Science,* 10(1), 104–115.
16. Donaldson, T. and Dunfee, T. (1994). Toward a Unified Conception of Business Ethics: Integrative Social Contracts Theory. *Academy of Management Review*, 19(2), 252-284.
17. Fried, C. 1968. "Privacy [A Moral Analysis]," in Philosophical Dimensions of Privacy: An Anthology, 203–23. Cambridge: Cambridge University Press.
18. Grama, J. (2020). Legal and Privacy Issues in Information Security. (3rd Edition). Burlington, MA. Jones & Bartlett Learning.
19. Kitchin, R. (2015). Making Sense of Smart Cities: Addressing Present Shortcomings. *Cambridge Journal of Regions, Economy and Society*, 8(1), 131-136.
20. Laufer, R. and Wolfe, M. (1977). Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. *Journal of Social Issues*, 33(3), 22-42.
21. Malik, A., Hiekkanen, K., Dhir, A. and Nieminen, M. (2016). Impact of Privacy, Trust, and User Activity on Intentions to Share Facebook Photos. *Information Ethics Society*. 364–382.
22. Miller, D. (2010). "Why Immigration Controls Are Not Coercive: A Reply to Arash Alizadeh," *Political Theory*, 38(1): 111–0.
23. Milne, G. and 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.
24. Morris., C. (1999). The Social Contract Theorists: Critical Essays on Hobbes, Locke, and Rousseau. Rowman & Littlefield Publishers.
25. Netanel, N. (2000). Cyberspace Self-Governance: A Skeptical View From Liberal Democratic Theory. *California Law Review,* 88(2), 395-498.
26. Perreault Jr, W. and Leigh, L. (1989). Reliability of Nominal Data Based on Qualitative Judgments. *Journal of Marketing Research*, 26(2), 135-148.
27. Punj, G. (2018). Understanding Individuals' Intentions to Limit Online Personal Information Disclosures to Protect Their Privacy: Implications for Organizations and Public Policy. *Information Technology and Management Journa*l.
28. Ritchie, D. (1891). Contributions to the History of the Social Contract Theory. *Political Science Quarterly*, 6(4), 656-676.
29. Steinfeld, N. (2016). "I Agree to the Terms and Conditions": (How) Do Users Read Privacy Policies Online? An Eye-Tracking Experiment. *Computers in Human Behavior*, 55, 992-1000.
30. 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.
31. Van Egmond, M., Spini, G., Van der Galien, O., IJpma, A., Veugen, T., Kraaij, W. and Kooij-Janic, M. (2021). Privacy-Preserving Dataset Combination and Lasso Regression for Healthcare Predictions. *BMC Medical Informatics & Decision Making*, 21 (1). 1–16.
32. Vile, J. (2021). A Companion to The United States Constitution and Its Amendments. Santa Barbara, CA. Praeger.