Shaffer, Gwen Lisa, 2025. "Trust, transparency and technology: Providing digital sovereignty through a 'Digital Rights Platform.'"
communication +1, vol. 11, issue 2, pp. 1—37.
DOI: https://doi.org/10.7275/cpo.2250

Trust, transparency and technology: Providing digital sovereignty through a "Digital Rights Platform"

Gwen Lisa Shaffer, California State University Long Beach, US, gwen.shaffer@csulb.edu

This article analyzes data collected during user testing of a community-informed "Digital Rights Platform" in Long Beach, CA. The Platform uses physical signage and an online portal to provide residents with a clear understanding of how local government applies predictive and diagnostic analytics to personal data. Grounded in theoretical frameworks of trust, surveillance studies and Contextual Integrity, this interdisciplinary project is motivated by the conceptualization of privacy as both a human right and a societal value. The research encompasses both theoretical and applied elements of digital sovereignty, and represents a praxeological investigation of digital sovereignty-related issues in the smart city context. The research's central questions explore how the Digital Rights Platform influences residents' attitudes toward and comfort levels with surveillance technologies deployed by the City of Long Beach. The study also examines whether—by providing transparency and accountability for City data collection—the Digital Rights Platform strengthens trust in local government or shifts power to residents. Both the theoretical and policy implications of this project are transferable and scalable to cities beyond Long Beach.

Introduction: Data privacy and the "smart" city

"Smart" cities promise higher quality of life for residents through data-driven insights. Local governments obtain these insights by subjecting residents to surveillance in all aspects of their lives. Routine daily tasks are no longer private because of technologies that collect real-time data, such as smart water meters that track shower lengths, traffic cameras that capture images of vehicles at red lights, municipal WiFi hotspots that automatically connect to smartphones, and parking apps that know a user's geolocation and credit card information. These intrusions into personal privacy call for a fundamental right to self-determination when interacting with digital technologies. Drawing from existing conceptions of digital sovereignty, this study considers it to mean an individual's ability to exercise autonomy and control over one's data and online content, including with whom digital personal information can be shared and used.[1] For smart city residents, the "participatory dimensions" of digital sovereignty "involve being able to strike one's own balance between shielding data and making it available in a controllable way."[2]

Municipal-level policymakers justify massive collection of personal information, arguing that such practices enable local government to efficiently deploy and manage city services—trash and recycling pick up, public safety initiatives, street design, and much more. Increasingly, however, residents question whether the benefits of smart city technologies outweigh the drawbacks associated with privacy violations and data breaches. For example, about 70 percent of U.S. adults recently reported feeling very or somewhat concerned about how the government uses data collected about them, up from 64 percent in 2019.[3]

These findings align with several previous studies conducted by our research team, comprised of researchers at California State University Long Beach and staff who lead the City of Long Beach's "Smart City Initiative." Since 2019, our team has examined residents' attitudes toward and comfort levels with civic technologies in the public realm. Findings from focus group discussions with 82 residents of Long Beach—the second largest city in Los Angeles County, with a population of about 500,000

[1] Reinhard Posch, "Digital Sovereignty and IT-Security for a Prosperous Society," edited by H. Werthner and F. Van Harmelen, *Informatics in the Future*. Proceedings of the 11th European Computer Science Summit (ECSS 2015), Vienna: 2015; Francesco Crespi, Serenella Caravella, Mirko Menghini, and Chiara Salvatori, "European Technological Sovereignty: An Emerging Framework for Policy Strategy," *Intereconomics* 56, no. 6 (2021): 348–54.

[2] Matthias Braun and Patrik Hummel, "Is digital sovereignty normatively desirable?," *Information, Communication & Society* (2024): 1–14.

[3] "Key Findings About Americans and Data Privacy," Pew Research Center, Last modified October 18, 2023, https://www.pewresearch.org/short-reads/2023/10/18/key-findings-about-americans-and-data-privacy/.

people—suggest that excessive surveillance reinforces a sense of insecurity and leads residents to fear civil liberties violations.[4,5] Members of Long Beach's BIPOC (Black, Indigenous and people of color) communities said they are particularly wary of surveillance technologies used by law enforcement, with automated license plate readers (ALPRs) and facial recognition technology cited as the most problematic. Further, when the City of Long Beach disseminated a survey designed to gauge attitudes toward smart technologies and data sharing, more than 80 percent of the 453 respondents reported feeling "strongly concerned" or "somewhat concerned" that the use of smart city technologies could mean less privacy for residents.[6]

Increasingly, local governments outsource functions to data-gathering companies whose business models are predicated upon surveilling residents and extracting personal information to serve their own business interests—which may include targeted advertising, analyzing user behavior and optimizing app functionality/services. As a result, our fundamental rights to privacy and autonomy are jeopardized, "and the trust and accountability deficit" is substantially growing.[7] We expect local government to provide services that enhance quality of life and boost accessibility. Instead, digitization and outsourcing have created a paradigm of extraction and exploitation, in which smart city residents are routinely "coded, quantified and rationalized to serve economic growth."[8]

For-profit companies that operate in California, even when based outside the state, are subject to the California Consumer Privacy Act (CCPA).[9] Theoretically, the CCPA shifts control away from corporations and empowers Californians to assume sovereignty over their own data. Specifically, the CCPA—and similar comprehensive data privacy laws enacted in 14 other U.S. states[10]—allows residents to opt out of data collection and request their personally identifiable information (PII) be deleted. But, in reality, powers granted under state statutes are impractical, as well as "too

[4] John Seberger and Gwen Shaffer, "Changing the Rules of Play in Long Beach, California: Smart Cities, Infrastructure and the Well-Played Game," *International Journal of Human-Computer Interaction* 39, no. 2 (2021): 1–16.

[5] Gwen Shaffer, "Applying a Contextual Integrity Framework to Privacy Policies for Smart Technologies," *Journal of Information Policy* 11 (2021): 222–65.

[6] Seberger and Shaffer, "Rules of Play," 6.

[7] Richard Whitt, *Reweaving the Web* (GliaNet Publishing, 2024), 17–18.

[8] Jason Moore, *Capitalism in the Web of Life: Ecology and the Accumulation of Capital* (Verso Books, 2015), 2.

[9] "Frequently Asked Questions," California Privacy Protection Agency, accessed November 13, 2024, https://cppa.ca.gov/regulations/pdf/cppa_act.pdf.

[10] "Which States Have Enacted Comprehensive Privacy Legislation?," *Bloomberg Law*, accessed March 18, 2024, https://pro.bloomberglaw.com/insights/privacy/state-privacy-legislation-tracker/.

fragmented and haphazard"[11] to meaningful protect data privacy. Further, government entities are exempt from compliance with the CCPA—a stipulation that blurs the lines between third-party vendor requirements and the lack of obligations placed on cities.

Rationale for the research

The current interdisciplinary research project is aimed at addressing these challenges. Our research team is designing and deploying a community-informed "Digital Rights Platform" that uses physical signage and an online portal to provide residents with a clear understanding of how local government applies predictive and diagnostic analytics to personal data. Grounded in theoretical frameworks of trust, surveillance studies and Contextual Integrity,[12] the Digital Rights Platform advances two critical and closely intersecting priorities for the City of Long Beach: implementation of its Data Privacy Guidelines[13] and its vision to use residents' data in non-discriminatory ways.[14] Specifically, the Digital Rights Platform is motivated by the conceptualization of privacy as both a human right and a societal value, and defines privacy as maintaining control over how one's PII is collected, used and stored.[15] The research encompasses both theoretical and applied elements of digital sovereignty, and represents a praxeological investigation of digital sovereignty-related issues in the smart city context. A key goal is to reduce (if not eliminate) the asymmetries that exist between governments and their third-party vendors—entities that extract personal information—and residents who must relinquish private details in order to participate in civic life. As noted by Seberger and Shaffer, "the smart city is imagined largely from the top-down, but it is lived primarily from the bottom-up."[16]

Between March 2, 2024 and March 9, 2024, our research team conducted user testing of the Digital Rights Platform with 77 residents. Each volunteer participated

[11] Daniel Solove, "The Limitations of Privacy Rights," *Notre Dame Law Review* 98 (2023): 975

[12] Helen Nissenbaum, "Privacy as Contextual Integrity," *Washington Law Review* 79, no. 1 (2004): 119–57, https://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf.

[13] "Data Privacy Guidelines," City of Long Beach, accessed February 1, 2024, http://longbeach.gov/globalassets/smart-city/media-library/documents/final_data-privacy-guidelines.

[14] "Framework for Racial Reconciliation," City of Long Beach, last modified June 26, 2020, https://longbeach.legistar.com/View.ashx?M=F&ID=8595273&GUID=107D5EFA-D10F-4444-B35A-3E7C272887BD.

[15] "Fostering Civic Trust: A Policy Guide for Municipal Leaders," U.S. Ignite, May 2021, https://www.us-ignite.org/wp-content/uploads/2021/06/USIgnite-CIVIC-Trust-Guide-Final.pdf.

[16] Seberger and Shaffer, "Rules of Play," 13.

in a focus group discussion, followed by a "data walk" and a second focus group discussion. This paper explores four central questions, emerging from our findings: 1) When interacting with and sharing personal information with city-deployed technologies, do Long Beach residents feel safer, watched, or violated? And by extension, how do these responses and attitudes influence residents' relationships with local government? Their relationships with public spaces? 2) By providing transparency and accountability for City collection of PII, does the Digital Rights Platform strengthen trust in local government and/or bolster comfort levels with civic technologies? 3) Does the Digital Rights Platform shift power from technology companies and local government to residents? And, finally, 4) What additional steps could empower residents and ensure agency over their personal information?

Both the theoretical and policy implications of this project are generalizable to cities beyond Long Beach. Our research team and City of Long Beach officials are committed to working cross-jurisdictionally to advance adoption of the Digital Rights Platform standard in peer municipalities.

How the paper is organized

The remainder of this paper is organized as follows: the subsequent section describes the rationale for designing and deploying a Digital Rights Platform. Next, the paper highlights relevant theoretical and legal approaches to data privacy—primarily, the frameworks of Contextual Integrity, cultures of trust and information economics, as well as the data walking methodology—in order to provide context for this project and introduce its foundational concepts. This is followed by an explanation of the methodology used for collecting user testing data and analyzing these data. The subsequent section discusses key findings and analysis emerging from our seven user testing events, including both political and policy-oriented implications. Specifically, it sheds light on how residents situate data collection by civic technologies, their expectations of local government, and routine privacy trade-offs—and what these findings mean for trust in local officials and for narrowing data asymmetries. The conclusion further discusses the implications of surveillance technologies in the civic realm and describes future research to advance project goals.

Digital Rights Platform: Design, objectives and implications

Long Beach's Digital Rights Platform consists of physical signs, or "privacy labels," featuring text and the open-source Digital Trust for Places and Routines (DTPR) iconography to visually convey which City-deployed technologies collect personally

identifiable information, how each device or software system collects those data, and the purpose of the data collection. Each label includes a unique QR code that, when scanned, takes users to a page on the online platform specific to the technology being encountered. That platform page presents additional details about collection of PII further down the DTPR "data chain," including how the City stores data from a specific device or app, who can access that data, which entity is responsible for the data, and more. Users may also leave comments and share concerns with government officials through the Digital Rights Platform portal.

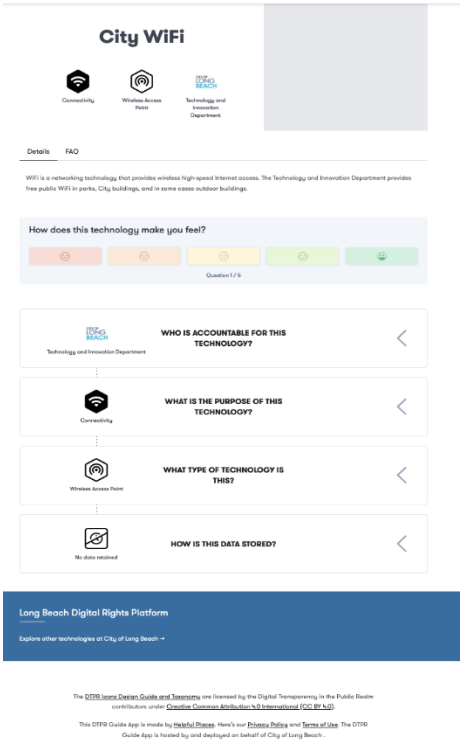
Figures 1, 2, and 3: Privacy labels posted adjacent to civic technologies.

As of February 2025, our research team had designed and mounted 22 privacy labels in three communities that reflect Long Beach's diverse population. These neighborhoods include Downtown, which is about 31 percent White, 33 percent Latinx/Hispanic, 18 percent African American and 15 percent Asian;[17] North Long Beach, which is 57 percent Latinx/Hispanic;[5] and Cambodia Town, home to an estimated 20,000 Cambodian residents.[18] Nearly all the 22 physical signs are printed on weather-resistant Dibond aluminum composite. (The exception is a data privacy label describing the Moovit mobile app, which is printed on a plastic cling that adheres to Long Beach Transit cashier windows and bus shelters.) The research team

[17] "Long Beach, Calif.," U.S. Census Bureau, accessed July 13, 2024, https://www.census.gov/quickfacts/fact/table/longbeachcitycalifornia/PST045222.

[18] "Race and Ethnicity in Downtown Long Beach, Calif.," Statistical Atlas, accessed July 13, 2024, https://statisticalatlas.com/neighborhood/California/Long-Beach/Downtown/Race-and-Ethnicity.

worked with a contractor to mount these data privacy labels physically adjacent to civic technologies, e.g., security cameras, mobile payment kiosks, public WiFi routers.



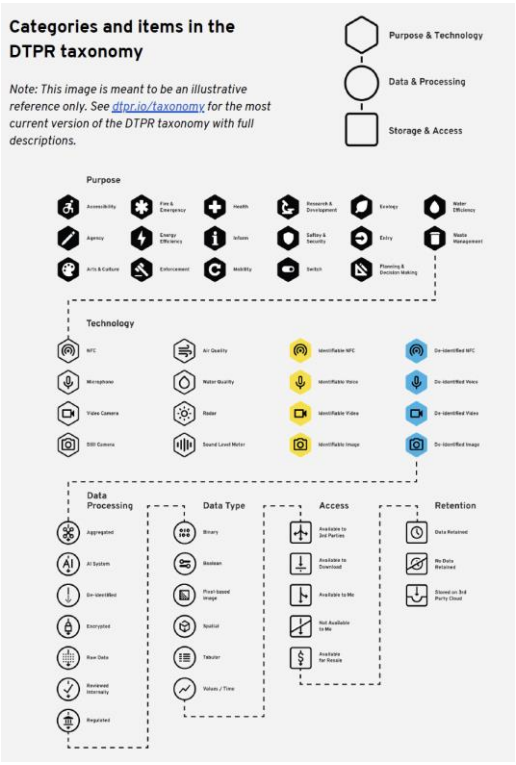


Figure 4 (left): Digital Rights Platform screenshot. Figure 5 (right): DTPR data chain.

Our research team also designed labels to digitally embed on the homepage of public computers used by library patrons and on the City's 311 mobile app in the future.

The following section examines literature from the fields of economic informatics, surveillance studies, law, and science and technology studies that informed our research questions, methodology and approach to data analysis.

Approaches to examining and understanding digital rights, and how they inform the current study

A Contextual Integrity framework

Levels of trust differ according to particular circumstances, such as: the types of data collected, how data are shared, and who has access to the information. Recognizing these variables, Nissenbaum[9] proposes a Contextual Integrity framework meant to

provide a holistic approach—drawing on scholarship situated in the law, public policy and political philosophy—for understanding privacy expectations and their implications. Nissenbaum asserts that privacy "is preserved when informational norms are respected and violated when informational norms are breached." Information flows within a delineated context that fail to adhere to existing norms are perceived as privacy violations. In the smart city context, an internet-connected water meter must record water consumption, as well as water pressure and flow, to identify leaky pipes; the app's functionality depends on access to these details. By contrast, a City deployed WiFi network does not need to store information regarding which websites a user visited; therefore, retaining users' browsing history constitutes a privacy violation.

Research I previously conducted offers a systematic and scalable approach to crafting local government privacy protections that conform to privacy norms, based on the theory of Contextual Integrity. The proposed model recognizes that local governments collect and process personally identifiable data in broad and distinct ways, from facial recognition software in airports to intelligent transportation tiles containing near field communication on subways. The study also demonstrates that qualitative data and survey responses can be used to test the conformity of existing privacy protections, corporate privacy policies and residents' notions of privacy norms.[19]

Detractors of Contextual Integrity point out that divergent life experiences and opposing political perspectives make it nearly impossible to find consensus surrounding what constitutes a norm. As sociologist James Rule writes, it may be reassuring to presume "that every social setting has unique, clear-cut standards governing 'appropriate' treatment of personal information" but, in reality, reasonable people disagree on this topic.[20] Additionally, Nissenbaum herself has acknowledged that ethical norms vary under transformations that take place along the "data chain." For instance, data provided for one's personal use (i.e., using an online calendar) take on new meaning when those data are shared directly with advertisers creating personalized ads.[21] Another critique of Nissenbaum's work points out that, by relying on a universal conceptualization of social norms, a Contextual Integrity framework "mismeasures" and even excludes the experiences of marginalized community

[19] Shaffer, "Applying a Contextual Integrity Framework," 222–65.

[20] James Rule, "Contextual Integrity and Its Discontents: A Critique of Helen Nissenbaum's Normative Arguments," *Policy & Internet* 11, no. 3 (2019): 260–79.

[21] Helen Nissenbaum, "Contextual Integrity Up and Down the Data Food Chain," *Theoretical Inquiries in Law* 20, no. 1 (2019): 221–56.

members.[22] Specifically, when sociotechnical norms are defined without input from vulnerable populations, who often hold competing values and experience unique realities, particular tensions around norms never get factored into the equation.

The present research acknowledges problems inherent in suggesting that uniform normative codes exist. Nevertheless, it maintains that Nissenbaum's Contextual Integrity framework serves a valuable function shaping data privacy standards. The current study aligns with McDonald and Forte's proposal to augment the Contextual Integrity framework by introducing vulnerability and centering diversity in "qualitative investigations of a population to understand important features like norms and information flow within a given context"[23]—as detailed later in both the Methodology and Findings and Analysis sections.

Information economics

The field of information economics[24] also influences our Digital Right Platform design. In particular, research on the effectiveness of Proposition 65, a California law requiring businesses to provide warnings about significant exposures to chemicals that cause cancer or other reproductive harm,[25] provides key insights. Because the Prop 65 list now includes nearly 900 toxins and carcinogens,[26] chemical warnings are omnipresent in California—from placards adjacent to artificial sweetener at Starbucks to stickers on furniture purchased at IKEA. There's a powerful argument to be made that these labels equalize negligible and severe risks,[27] and that the warnings are easily ignored. The Digital Rights Platform design recognizes that posting data privacy labels on every civic technology throughout a city could result in a comparable "privacy fatigue." Another take-away from Prop 65 is that some product manufacturers have reformulated their products with safer ingredients, rather than place fear-inducing warnings on them. As our research team scales the Digital Rights Platform and data privacy labels become more widespread, our research team will

[22] Nora McDonald and Andrea Forte, "The Politics of Privacy Theories: Moving from Norms to Vulnerabilities," in CHI '20 Proceedings, (Honolulu, 2020), 5.

[23] McDonald and Forte, "Politics of Privacy," 9.

[24] Kenneth Arrow, "The Economics of Information: An Exposition," *Empirica* 23 (1996): 119–28.

[25] Ganda Suthivarakom, "Wirecutter: What is Prop 65? And Why Is There a Warning Label on This Thing I Bought?," *New York Times*, March 10, 2020, https://www.nytimes.com/wirecutter/blog/what-is-prop-65/.

[26] "Proposition 65," California Office of Environmental Health Hazard Assessment, accessed July 13, 2024, https://oehha.ca.gov/proposition-65.

[27] Michael Barsa, "California's Proposition 65 and the Limits of Information Economics," *Stanford Law Review* 49, no. 5 (1997): 1223–47.

monitor for similar impacts. Future research questions will explore whether tech companies that contract with the City of Long Beach limit data collection in order to avoid data privacy labels being placed near their devices.[28]

Similar to Long Beach's data privacy notices, other scholars have explored communicating the ways organizations collect, use, and share personal information through visual language. Perhaps most notably, Kelley, Bresee, Cranor and Reeder prototyped privacy labels that provide consumers with a "clear, uniform, single-page summary of a company's privacy policy."[29] Akin to nutrition labels found on food packaging, their design is meant to reduce "wiggle room and complicated terminology by using four standard symbols that can be compared easily."[30] Following user testing with 24 participants, the researchers identified multiple benefits of disclosing data privacy information in the format of a "nutrition label" versus natural language. For example, users noted the benefits of being able to find information in the same place every time; to ascertain key points simply by looking at the overall intensity of the page; to print the data privacy disclosure; and to fit the entire disclosure in a browser window. These findings demonstrate the potential societal value of displaying data privacy labels adjacent to civic technologies deployed by the City of Long Beach (and, in the future, other municipalities).

Daniel Susser's decoupling of notice-and-consent provides another strong rationale for the Digital Rights Platform. Susser characterizes the notice-and-consent regime currently dominating online privacy as "an illusion" but goes on to assert that *disclosures* effectively help users make informed choices.[31] Similarly, our research examines whether the Digital Rights Platform signage creates "basic situational awareness"[32] about key information, i.e., whether a smart technology stores PII or sells it for targeted advertising. In particular, Susser's ideas inform our second research question, which hypothesizes that, by providing transparency and accountability, the Digital Rights Platform may bolster residents' confidence in both local government and civic technologies.

Within the context of smart city technologies, a certain amount of data collection is necessary. Shared scooters and bikes, library book check-out kiosks, and online utility bill payments are examples of services that require (some combination

---

[28] Barsa, "Prop 65."

[29] Patrick G. Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder, "A 'Nutrition Label' for Privacy," Symposium on Usable Privacy and Security Proceedings, (Mountain View, 2009), 1.

[30] Kelley, et al., "Nutrition Label for Privacy," 11.

[31] Daniel Susser, "Why Privacy Disclosures are Valuable Even if Consent Frameworks are Not," *Journal of Information Policy* 9, April 18, 2019: 148–73, 154.

[32] Susser, "Privacy Disclosure," 164.

of) geolocation, credit information and energy consumption. However, the typical data privacy policy for these services fails to recognize the contextual variables that Nissenbaum articulates. [33] By providing details about how the City of Long Beach collects and uses residents' data, the Digital Rights Platform aims to ensure residents can make informed decisions about civic technology use. And, as the Digital Rights Platform evolves, our research team is designing functionality meant to give residents more agency over how their data is collected and used—plans elaborated on in the Conclusion.

Existing data privacy laws: Protections and shortcomings

While the United States lacks a comprehensive federal data privacy law, about 15 U.S. states, including California, have stepped in to fill the void. Legal scholar Daniel Solove argues that the "individual rights" integral to these privacy regulations are far less capable of advancing personal data privacy protections than policymakers assume.[34] Solove points out that granting rights shifts much of the onus to individuals, when privacy problems tend to be systematic. Additionally, making difficult decisions about personal privacy requires time and expertise, both of which most people lack. Relatedly, it is impractical to exercise data privacy rights "at scale," given the countless organizations that process our data. Both anecdotal evidence and academic research have established that most online users accept terms of service agreements without reading or understanding them.[35] Finally, Solove stresses that an individual's personal data is actually part of a larger data ecosystem, mandating that privacy protections be broadly focused, as opposed to aimed at individuals. [25]

In its current iteration, the Digital Rights Platform requires Long Beach residents to consider their data privacy while engaged in some other primary task, i.e., browsing the internet at the library or passing by a public safety camera. Findings emerging from our user testing events—discussed in detail later—bear out Solove's concerns. As our research team refines and scales the Digital Rights Platform, we are incorporating elements that transcend data rights and move users closer to true digital sovereignty.

---

[33] Nissenbaum, "Contextual Integrity," 119–57.

[34] Daniel Solove, "The Limitations of Privacy Rights," *Notre Dame Law Review* 98 (2023): 975.

[35] Aindrila Chakraborty, Ramesh Shankar, and James Marsden, "An Empirical Analysis of Consumer-Unfriendly E-commerce Terms of Service Agreements: Implications for Customer Satisfaction and Business Survival," *Electronic Commerce Research and Applications* 53 (2022): 101151.

Previous research on the DTPR standard

The Digital Rights Platform's key design elements are based on the work of Helpful Places. This consultancy advances the adoption of DTPR, a communication standard centered around icons meant to quickly and clearly convey a "data chain." This encompasses the entity responsible for the data collection, the purpose of the data collection, who can access those data, and how data are stored. In 2022, Helpful Places analyzed DTPR pilot projects with four municipalities: Angers Loire Metropolitan Region in France; the Town of Innisfil in Canada; Boston; and Washington, DC.[36] Across these cities, Helpful Places deployed a total of 48 signs representing 13 distinct technologies. In its analysis of feedback on DTPR signage from nearly 1,400 people, Helpful Places notes the importance of developing a communications and engagement plan early on. With this in mind, our research team has formed an array of partnerships with community-based social service organizations, neighborhood groups, privacy advocates and legal experts.

Helpful Places' evaluation of user feedback also underscores the need to consider both foot traffic and the availability of mounting locations when determining where to place data privacy notices. These details influenced our research team's decision to include or exclude certain smart city technologies in the Digital Rights Platform deployment. Finally, Helpful Places' analysis of its four pilot deployments highlights the importance of ensuring buy-in from key stakeholders. [27] In recognition of this finding, our research team hosted a "digital rights 101" workshop in September 2023 that introduced key City subject matter experts to broad concepts of data privacy and laid out the rationale for the Digital Rights Platform. Representatives from the Long Beach Police Department, the Department of Public Works, the Department of Technology and Innovation, the Health and Human Services Department, Long Beach Transit, and the Public Library participated in this workshop.

Data Walking as a theory and as a methodology

Our project is also informed by previous studies that employ data walks—which function as both a methodology and an analytical framework. Data walks embody an interdisciplinary approach that integrates communication studies, technology studies

[36] "2022 DTPR City Cohort Program Report," Helpful Places, https://medium.com/@helpfulplaces/helpful-places-releases-2022-dtpr-city-cohort-program-report-a00a40dee736.

and urban planning to examine the increasing datafication of our lives.[37] As study participants cross paths with civic technologies like public WiFi hotspots and traffic cameras, they gain a heightened awareness of just how much PII is generated by routine tasks. During walks through various sections of Rotterdam and The Hague in the Netherlands, van Zoonen[38] and her colleagues asked 70 study participants, including some municipal workers, to contemplate where they saw data and what they believed happened with it. Relevant to the concept of digital sovereignty, the researchers asked volunteers to also consider who owns data and whether they would prefer to have some say about it. Discussions during these data walks led van Zoonen et al.[28] to conclude that neither residents nor city employees seriously reflect on the immense role data collection plays in their lives, and that digitization must be reconstructed "as a social issue rather than as an individual responsibility."[29]

Data researcher Allison Powell led "data walkshops" for multiple collaborations with British artists, urban planners, activists and workers. Powell aptly characterizes this methodology as "a radically bottom-up process of exploring and defining data, 'big data' and data politics" from the perspectives of residents.[39] Powell views walkshops as "especially powerful in connecting questions, concerns or investigations related to data" with prevailing social challenges. For example, her urban treks exposed participants to issues ranging from racial inequities and environmental degradation, to food deserts and homelessness.[40] Analogously, volunteers in the Long Beach walks crossed paths with unhoused residents along all three neighborhood routes, and encountered just one super market (during the Downtown route).

The scholarly literature described in this section informed our theoretical approach and the central questions guiding the current study. Next, the paper describes how members of my research team and I recruited study participants; designed the methodologies employed for collecting study data; and analyzed those data.

---

[37] Karin Van Es and Michiel de Lange, "Data With its Boots on the Ground: Data Walking as a Research Method," *European Journal of Communication* 35, no. 3 (2020): 278–89.

[38] Liesbet van Zoonen, Fadi Hirzalla, Jiska Engelbert, Linda Zuijderwijk, and Luuk Schokker, "Seeing More Than You Think: A 'Data Walk' in the Smart City," in *Public Engagement with the Smart City*, ed. S. Hussey (Bang the Table, 2017), 16–19.

[39] Allison Powell, "Data Walks and the Production of Radical Bottom-up Data Knowledge," paper presented at the International Communications Association conference, San Diego, California, May 24, 2017: 2.

[40] Ibidem, 3.

Methodology

Data collection

Between March 2 and March 9, 2024, our research team facilitated seven user testing events to assess efficacy of the Digital Rights Platform's physical privacy labels and its online platform. We disseminated recruitment flyers (in English, Spanish, Khmer and Tagalog) through community-based organizations; newsletters from the Long Beach mayor; district updates shared by all nine City Council members; the Long Beach Technology and Innovation Department newsletter; local media outlets; and a study recruitment website. As noted on the flyers, volunteers were offered a $25 gift card for participating in two focus group discussions and a data walk—a combined 2-hour commitment.

Figures 6, 7 and 8: User testing recruitment flyers in English, Spanish and Khmer.

About 110 people registered through a Microsoft Forms survey that enabled them to choose their preferred date and time, based on nine potential time slots. The form also collected basic demographic information, including age, ethnicity, gender, education level, annual income and zip code. In addition, the questionnaire asked volunteers if they required language translation services or accommodations (i.e., a wheelchair, a tablet computer). Several days prior to the start of each walk, I sent a confirmation email to registered volunteers. The message provided directions and parking information for the neighborhood library where their specific user testing event would begin, and contained a link to a custom version of the Jotto mobile app they would need for responding to prompts during the data walk.

In terms of education levels, 27 registrants reported earning a bachelor's degree; 26 reported earning a masters or doctorate degree; everyone else reported having attended "some high school" or "some college." Incomes reported by those who registered were evenly distributed among those with high annual household incomes ($91,000 or more), middle annual household incomes ($61,000 to $90,000) and lower income earners ($31,000 to $60,000). The exception was registrants for one Cambodia Town walk, where a vast majority of participants reported annual incomes of less than $30,000. These charts reflect self-reported ethnicity, age and gender of study volunteers:

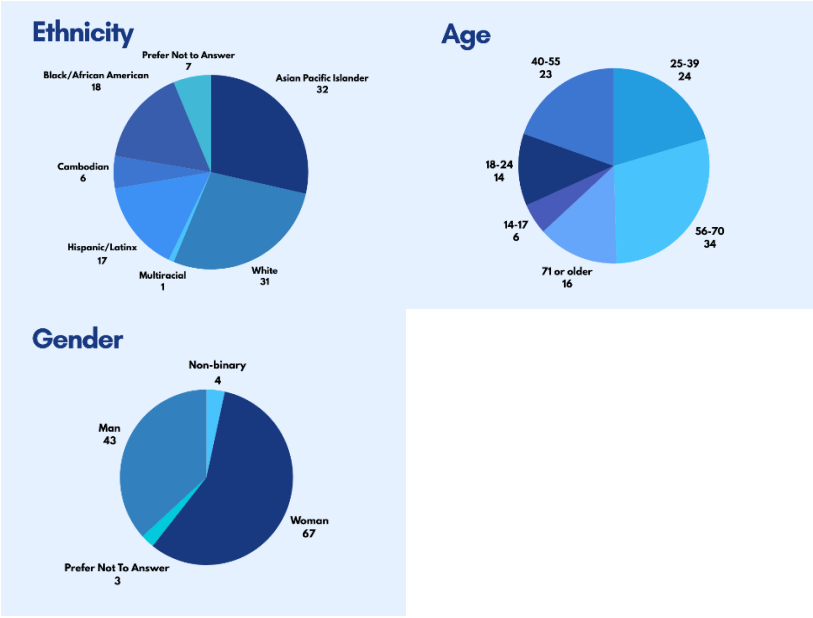
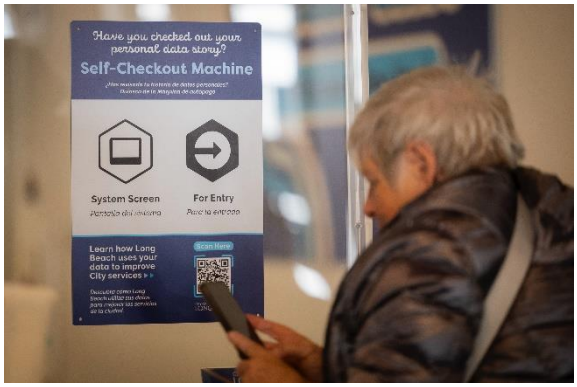


Figure 9: Ethnicity, age and gender of user testing.

Ultimately, 77 people participated in a total of seven user testing (cool, rainy weather throughout the week likely discouraged some registrants from attending). Upon arriving at the neighborhood library, research team members asked each volunteer to review and sign an informed consent document, and I explained the purpose of the study. The group then engaged in a semi-structured discussion—lasting between 20 and 30 minutes—meant to sensitize volunteers to the general topic of data privacy. Our conversations explored participants' generic privacy concerns and steps they take, if any, to protect their data. Conversations then delved into impressions of technology use by the City of Long Beach. Before heading out for each walk, I asked participants what they expected to see.

While traversing routes in the North Long Beach, Cambodia Town and Downtown neighborhoods, study participants encountered privacy labels adjacent to public Wi-Fi routers, docking stations for bikes and scooters, automated license plate readers (ALPRs), parking payment kiosks, library self-checkout machines, internet-connected bus stops, smart water meters, public computers, and security cameras.



Figures 10 and 11: Data privacy labels adjacent to a library self-check kiosk and a Passport Parking payment kiosk.

Study participants used the Jotto app to respond to these questions each time they encountered a smart city technology:

1. What type of data do you believe this smart technology collects?
2. Does the technology in our built environment stand out more than prior to our discussion?
3. How comfortable are you sharing personal information while using/interacting with this particular technology?

4. Anything else you would like us to know, regarding how you feel about this smart technology?
5. What is the data privacy notice telling you, and is it placed in a location that catches your attention? Please explain the reason for answering yes or no.

Each walk lasted approximately 45 minutes. Participants then returned to the library, where I facilitated a "debriefing" focus group discussion that centered around these prompts:

1. Were you surprised by anything you observed during the walk?
2. Is it the City's responsibility to inform residents about data collection, or are residents responsible for their own awareness of the "smart" technologies Long Beach deploys?
3. Do the benefits of data collection, such as traffic management, outweigh potential privacy violations?
4. Do the civic technologies we observed make you feel safer, watched, or violated?

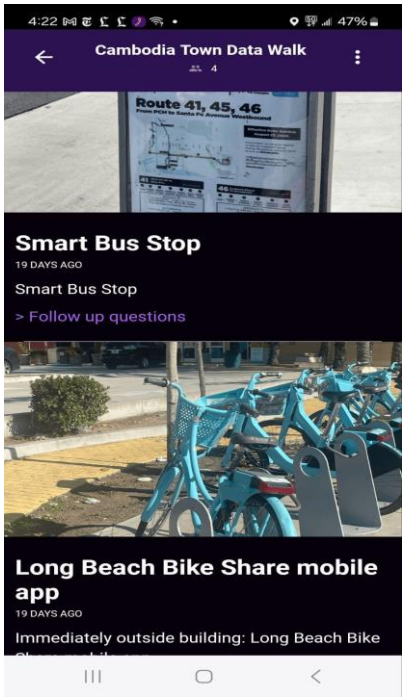


Figure 12: Screenshot of Jotto mobile app.

Data collection

Study participants submitted a total of about 800 video, audio and text comments through the Jotto mobile app. Artificial intelligence embedded into Jotto transcribed video and audio comments. A research assistant used the software TurboScribe.ai to transcribe the focus group discussion recordings. I then reviewed each transcript for accuracy and corrected errors by listening to the audio/video submitted through Jotto and to focus group recordings.

For the analysis, I relied on abductive analysis—an inferential process aimed at producing new hypotheses and theories emerging from "surprising" research evidence[41]—in which themes emerged from the text of the pre- and post-walk interview transcripts and responses submitted to the mobile app. Specifically, I linked discourses of data privacy violations, trust, comfort levels and transparency with a critical perspective on smart city technologies and data privacy labels. I then systematically coded the qualitative data (consisting of transcripts from the 14 focus group discussions and approximately 800 Jotto comments). A research assistant and I separately read each transcript multiple times to form a systematic analysis through the lens of Nissenbaum's[42] Contextual Integrity framework, as well as theories associated with information economics, surveillance studies and cultures of trust literature. Through further abductive analysis, we related data to ideas, then ideas to other ideas. The research assistant and I used the qualitative data analysis platform Nvivo 14 to separately code the transcripts according to thematic relevance. After initially identifying a dozen "nodes," we compared them against the conceptual arguments supporting this study and our research questions. I then analyzed and revisited these themes, using techniques that are cyclical and iterative. Through this process, we determined that some nodes were less significant or redundant, ultimately resulting in six key themes.

Findings and analysis

This research recognizes that technologies retain and grant power—and that a power imbalance exists between cities deploying surveillance tools (along with third-party vendors), and the residents subject to their capabilities to monitor, gather and store information. Therefore, the analysis of our study findings embody both political and

[42] Iddo Tavory and Stefan Timmermans, *Abductive analysis: Theorizing qualitative research* (The University of Chicago Press, 2014).

[42] Nissenbaum, "Privacy as Contextual Integrity."

policy implications.[43] Idealized notions of digital citizenship, as well as characterizations of technology as impartial and value-neutral, gloss over the role technology plays in both our personal and public lives. These ideas are central to the study analysis.

The role of technology functionality and perceived trade-offs in determining residents' feelings and attitudes

A guiding question for this research asks if Long Beach residents feel safer, watched, or violated when interacting with and sharing personal information with city-deployed technologies. Based on analysis of the findings from user testing, the answer to this enquiry is highly contextual and variable. By contrast, one finding remains consistent: the existence of a power differential between technology users, and City government/third-party vendors that develop and deploy smart technologies. Tech companies are motivated by profits and they yield far-ranging influence. Combined, these realities sustain the current online paradigm characterized by data "surveillance, extraction, analysis and manipulation."[44]

Through apps and smart devices that make users feel connected and in control, developers of civic technologies exert very real power. Users come to expect, and even depend on, the instant gratification and convenience of these technologies. Based on comments from many of our study participants, emotional and pragmatic rewards tend to eclipse feelings of being violated or watched. For example, study participants in all seven user testing events referenced a November 2023 cyberattack against the City of Long Beach. (Ransomware attackers target local government entities more than any other sector, with the exception of academia[45]). Volunteers commented that the incident—which forced the City to go offline for two weeks and to acknowledge stolen data[46]—shook their faith in the City's ability to keep PII safe. "As embracing of technology as I am, I would never connect to public WiFi, especially after the City of Long Beach's site was hacked," a study participant said. The data breach made one resident wonder if criminals obtained his credit card number, bank

[43] Akwugo Emejulu and Callum McGregor, "Towards a Radical Digital Citizenship in Digital Education," *Critical Studies in Education* 60, no. 1 (2019): 131–47, https://doi.org/10.1080/17508487.2016.1234494.

[44] Richard Whitt, *Reweaving the Web* (Glianet, 2024).

[45] "Ransom Attacks Straining Local U.S. Governments and Public Services," Federal Bureau of Investigation, March 30, 2022, https://www.ic3.gov/Media/News/2022/220330.pdf.

[46] Mekahlo Medina, "City Confirms Data Was Stolen in Cyberattack," *NBC Los Angeles*, November 29, 2023, https://www.nbclosangeles.com/local-2/city-of-long-beach-confirms-data-was-stolen-in-cyberattack/3279847/.

information and address, adding, "I was concerned." Another study volunteer noted that "our water, our sewer, our refuse…all that information is out there." Someone else characterized the cyberattack as "scary" because the Port of Long Beach plays a critical role in global commerce: "Any type of data, as innocuous as it might seem, can cause a major problem."

Yet, feelings of being watched and even violated as a result of the cyberattack on the City of Long Beach are contradicted by another reoccurring theme that emerged during user testing—a willingness to swap privacy for convenience. During focus group discussions and in comments submitted through the Jotto app, study participants alluded to consciously relinquishing personal privacy in exchange for the benefits of paying utility bills online, reporting potholes through the GoLongBeach app, and checking the bus schedule on the Moovit app, among other routine tasks. Notably, a majority of study volunteers reported feeling ambivalent about these trade-offs. For example, one focus group participant expressed alarm over ALPRs in City-owned parking garages, but immediately conceded that she appreciates quickly exiting the parking structure. "I'm happy to give my personal information to simplify the parking process…it just makes life easier," she said. Similar sentiments surfaced around various civic technologies, including comments like, "Meh. It feels intrusive but I get why we need it," and "I'm ok sharing my information for the convenience of having WiFi." Other respondents characterized data collection through surveillance technologies as "a necessary evil" and as "collateral damage to living in today's society." This last comment, submitted to the Jotto app, was accompanied by a shoulder shrug emoji.

The data privacy notices and online platform that comprise Long Beach's Digital Rights Platform are meant to tilt the power differential between civic technology developers and residents, which enables dataveillance. The study findings make clear that residents strongly support this goal. At the same time, however, volunteers expressed two main rationales for relinquishing control over their PII when interacting with City-deployed devices and platforms. Most prominently, they said sharing their personal data is necessary in order to further societal goods (i.e., public safety, streamlining of services, urban planning) and for convenience (i.e. saving time, simplifying tasks). "If it helps the city operate more efficiently or ultimately keeps me safer, my neighbors safer, I'm okay with what feels like a pretty small loss," a volunteer said. During another focus group discussion, a participant noted, "It's a little concerning that they're just recording us and everything that we do, where we are, what we're wearing, what we buy. But it comes for the price of safety." And a Jotto user acknowledged feeling "a bit uncomfortable" being recorded by security cameras

while checking out library books, "but I understand that it is for the better of the library."

Implicit in study participants' comments is the notion articulated by Rob Kitchin that "the mass generation of data about customers is cast as a choice between creating safer societies or defending personal autonomy."[47] Similarly, study participant comments echo the tech industry's insistence that innovation, customer experience and economic growth rely on data extraction.[48] Returning to our guiding question of whether Long Beach residents feel watched, violated or safe while interacting with surveillance technologies deployed by the City, the answer seems to be, "Yes." Our findings reveal a significant contradiction: Residents resent the invasive nature of civic technologies and are wary of them. But, at the same time, our study found that many people believe dataveillance—the use of PII in surveillance activities[49,50]— is necessary for maintaining public safety and conveniences they value. These findings suggests residents' interactions with sensors and the like are "multifaceted, contradictory and ambiguous."[51] They also align with previous research concluding that people value the benefits of smart devices enough to set aside privacy concerns associated with the data they collect.[52]

In fact, Americans engage in "interpersonal surveillance"[53] daily. We assign stars to our Uber drivers; we evaluate actors and directors through the "Tomatometer"; we assess authors on GoodReads; students essentially grade their instructors on RateMyProfessor. Often, people associate this interpersonal surveillance with trust, and believe it encourages citizens to obey rules and act honestly. However, as economist Rachel Botsman explains, the problem is that *government* surveillance "is a deeply disturbing version of reputation economics that

---

[47] Rob Kitchin, *Getting Smarter About Smart Cities: Improving Data Privacy and Data Security* (Dublin, Ireland: Data Protection Unit, Department of the Taoiseach, 2016), 47.

[48] Bruce Schneier, "How We Sold Our Souls–and More–to the Internet Giants," *The Guardian,* May 17, 2015, https://www.theguardian.com/technology/2015/may/17/sold-our-souls-and-more-to-internet-giants-privacy-surveillance-bruce-schneier.

[49] Jose van Dijck, "Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology," *Surveillance & Society* 12, no 2 (2014): 197–208.

[50] Sara Degli Esposti, "When big data meets dataveillance: the hidden side of analytics," *Surveillance & Society* 12, no. 2 (2014): 209–25.

[51] Chris Salter, S*ensing Machines: How Sensors Shape Our Everyday Life* (The MIT Press, 2022), 10.

[52] Adnan Chawdhry, Karen Paullet, and Jamie Pinchot, "Internet of Things: Measuring Data Privacy Concerns of Users," *Issues in Information Systems* 23, no. 4 (2022): 94–110.

[53] Rachel Botsman, *Who Can You Trust? How Technology Brought Us Together and Why It Might Drive Us Apart* (New York: Hatchette Book Group, 2017).

will give governments unprecedented control over what they consider good and bad ways to behave."[54] The following section delves into relevant implications.

How surveillance shapes residents' relationships with local government and public spaces

This project seeks to better understand how dataveillance enabled by civic technologies shapes residents' relationships with local government, and influences how they move through public spaces. Of note, BIPOC study participants in all seven user testing events spoke in personal terms about how dataveillance influences their relationship with local government and their interactions with specific City-deployed devices. Given that nearly a quarter of Long Beach residents were born outside the United States and non-citizens comprise more than 12 percent of the city's population,[55] this finding has substantial implications for understanding how trust is both fostered and eroded.

The "Black Opticon" is a phrase Anita Allen coined to signify the ways in which governments (and corporations) have monitored Black people and their data online[56] throughout U.S. history. Indisputably, Americans of color have long faced discrimination. But newer invasive technologies make it possible for government to operationalize racial biases through oversurveillance of particular communities. Geolocation tracking, biometric recognition tools and targeted surveillance of lawful protesters—such as widespread police monitoring of Black Lives Matter activists[57]—"are paramount data-privacy practices disproportionally impacting African Americans," Allen writes.[58]

Immigrants living in the United States are also intimately familiar with dataveillance. In her book exploring how undocumented Latinx families navigate life

---

[54] Botsman, *Who Can You Trust?* 170.

[55] "Long Beach, CA. Population and Diversity," Data USA, accessed July 15, 2024, https://datausa.io/profile/geo/longbeach-ca.

[56] Anita Allen, "Dismantling the 'Black Opticon': Privacy, Race, Equity and Online Data-Protection Reform," *The Yale Law Journal* 131 (2021), https://www.yalelawjournal.org/forum/dismantling-the-black-opticon.

[57] Matt Cagle, "Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color," *ACLU of Northern California*, October 11, 2016, https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target.

[58] Allen, "The Black Opticon."

under pervasive government surveillance, Asid Asid[59] describes how immigrants feel compelled to "selectively engage" with "mainstream" institutions that regularly surveil them. Asid describes how, during their first few years in the United States, immigrants typically avoid institutions that could connect them with health care, public assistance and education. When undocumented immigrants need to request government support, though, it comes with a cost: persistent monitoring. Asid makes sense of this selective engagement, which is fraught with inherent contradictions, by considering Foucault's[60] theory that surveillance encompasses facets of both risk and reward.

Both the Black Opticon and the undocumented immigrant experience of living on the radar of government agencies provide context for analyzing how dataveillance influences Long Beach residents' relationships with local government and public spaces. During multiple focus group discussions, participants mentioned how the Long Beach Police Department shared data from ALPRs with Immigration and Customs Enforcement during a 10-month span in 2020. This occurred despite a 2018 ordinance barring local agencies from providing information to federal immigration officials.[61] Years later, the violation—which the City maintains was inadvertent—continues to stoke anger and fear. "The immigrant community has been begging for years to remove this technology and I am horrified that it is still up, and at risk of being used by police," a study volunteer commented. Another focus group participant said that self-checkout kiosks in the libraries, for example, don't bother him "at all." By contrast, he is disturbed by the City of Long Beach's use of ALPRs:

> I think it's a small convenience at the expense of potentially the police getting that data and using it to target undocumented folks—which there is a real history of happening. And I don't think that most people are aware of that because it's sort of swept under the rug except for the community groups who are begging for somebody to do something about it. When you think about that as a trade-off… the half-second that I save by not taking out my parking ticket and [inserting it in a payment kiosk], compared to just driving out…If that is weighed against somebody getting deported in my community, are you kidding me?

---

[59] Asid Asid, *Engage and Evade: How Latino Immigrant Families Manage Surveillance in Everyday Life* (Princeton University Press, 2023).

[60] Graham Burchell, Colin Gordon, and Peter Miller, *The Foucault Effect: Studies in Governmentality* (Chicago, Illinois: University of Chicago Press, 1991).

[61] Kevin Flores, "City Council to Decide Whether to Buy Controversial License Plate Readers," *For the*, November 17, 2020, https://forthe.org/journalism/license-plate-readers/.

Lingering suspicion from the 2020 data breach percolated during other focus group discussions, and elicited lengthy conversations. For example, one study participant commented:

> I've been informed there is a chance that the license plate retrieval information is being used to cross reference people who might be undocumented. If that is even a remote possibility, I'm fully against this…I don't want any kind of extraction from that to hurt anyone else. If someone is driving a car and they're not crashing into anything, they're fine with me. I don't care where they're from or if they even have a driver's license.

Study participants criticized civic technologies for reasons beyond dataveillance, including several who pointed out that digitized city services exclude non-English speakers. A woman who works for a non-profit organization that advocates for Latinx rights said she is "totally" worried about people who don't "speak the language" and who are not "technology savvy." She commented: "My organization deals with a lot of Latino families and they don't have computers. They don't even know that they have email on their phones. The gap that these new technologies is creating is increasing, and I think there is a large, large community that we're leaving behind." She underscored this point with an anecdote: "We partnered with the City for rent relief and in order for me to help [our clients], I had to teach them how to use the phone."

A study participant who serves as president of an organization focused on the rights of older Americans rang a different alarm bell, noting that Long Beach has a "considerable" population of residents over the age of 70. "Those are people who probably, even during their work lives, had very little if any interaction with technology. So they're less apt to engage with a GoLongBeach app. They will just walk past those QR codes [on the Digital Rights Platform signage] and not even know what they are, right?"

These observations highlight the structural reality that City-deployed technologies disproportionately impact residents—depending on their race, ethnicity, age and socio-economic status. As study participants highlighted, surveillance technologies deepen the power imbalance between law enforcement officials and undocumented residents.[62] The mere perception of abuse is likely to erode

[62] Maša Galič, "Smart Cities as 'Big Brother Only to the Masses': The Limits of Personal Privacy and Personal Surveillance," *Surveillance & Society* 20, no. 3: 306–11, https://ojs.library.queensu.ca/index.php/surveillance-and-society/index.

institutional trust and even threaten social stability.[63, 64, 65] Further, concerns about data discrimination exemplify the ways in which smart technologies lead to privacy trade-offs that blend the tangible (the ability to hop on a shared bicycle or take advantage of internet connectivity at the park) with the intangible (the psychological discomfort experienced when your license plate is scanned or your water consumption is known in granular detail), and the incommensurable (the societal ramifications of surveillance; the loss of autonomy you experience when local government knows so much about you).[66]

"Rather than connecting the urban environment seamlessly and inclusively, as the smart city narratives promise," digitization separates and filters the population "along the lines of class and social agency."[67] Comparing comments made by BIPOC and white study participants underscores how government data collection is experienced differently by distinct populations. Specifically, white study participants, generally, characterized devices and platforms deployed by the City of Long Beach as simply part of a ubiquitous surveillant culture. As one volunteer said, "When I step out into the street, I don't distinguish between what is part of the city and what's private. I think I'm just being watched or information is being collected." Similar statements reflecting this viewpoint that surveillance is unavoidable include:

- "I feel like I'm so laissez faire about my data. I guess it's because everybody is asking for it."
- "I think all my information is out there already. I think it's just a big, messy place and anything you do online will get leaked."
- "Do you have a choice? Do you have an option? Do you have a bill to pay?"
- "It amazes me. I heard that when you walk out of your house, you're videotaped 18 times per day. If you go anywhere, whether that's a grocery store, a gas station, a department store…somebody is looking at you while you're all going through your city, taking care of your errands."

---

[63] Tom Julsrud and Julie Krogstad, "Is There Enough Trust for the Smart City? Exploring Acceptance for the Use of Mobile Phone Data in Oslo and Tallinn," *Technological Forecasting and Social Change* 161 (December 2020): 120314.

[64] Lynne Zucker, "Production of Trust: Institutional Sources of Economic Structure, 1840-1920," in *Research in Organizational Behavior*, ed. B. Staw and L. Cummings, vol. 8 (JAI Press, 1986), 53–111.

[65] Russell Hardin, *Trust* (Cambridge: Polity Press, 2006).

[66] Alessandro Acquisti, Curtis Taylor, and Liad Wagman, "The Economics of Privacy," *Journal of Economic Literature* 54, no. 2 (2016): 442–92.

[67] Antenucci, "Smart Cities, Smart Borders," 54.

- "I don't really think about how to minimize my footprint. I kind of assume it's just all out there, really."
- "If you have an issue with [being recorded], I guess you need to stay in the privacy of your own home. Or be aware that someone, somewhere is gonna capture what you're doing at some point."
- "Nowadays, almost everything you use—your credit card, your address and other identifying information—is stored."
- "I kind of work from the assumption that everything that is to be known about me is known already."

These comments reveal that a subset of residents do not differentiate between civic technologies in the public realm and, for example, a Google assistant on their kitchen counter or ChatGPT. In reality, though, critical differences exist in terms of the ability to opt-out of data collection and how data are used. Individuals committed to preserving data privacy can avoid shopping online, eschew social media, erase browser search histories, and turn off phone geolocation tracking. However, privacy settings are nonexistent in the context of most smart city technologies. For instance, residents routinely drive through intersections with municipality-owned traffic cameras and pass by police vehicles equipped with ALPRs. Even when residents are aware of devices capturing their image, they cannot toggle a button to reject cookies, adjust default privacy settings or submit an opt-out form. Several study participants who said they *do* distinguish between publicly and privately deployed surveillance technologies indicated that they place greater trust in corporations. "One of the issues for me, or something that I think about in this area, is that I've been conditioned to give private industry my information in exchange for the utilization of apps. However, when it comes to a government entity asking me to give my information, then in my mind it kind of becomes a different trade-off." Another focus group participant similarly asserted, "This government has way too much personal information and it can be held against you in many different ways."

A certain irony is evident here, given that private corporations routinely demonstrate their willingness to violate user privacy. As Shoshana Zuboff observes, we truly are living in an unprecedented time, when the wealthiest corporations have access to "a pervasive global architecture of ubiquitous computation," resulting in "unparalleled concentrations of information" about individuals and populations. Corporations capitalize on these granular insights to manipulate people into foregoing their own best interests and, instead, behave in "commercially desirable"

ways. [68] In one high-profile example of corporate data exploitation, General Motors sold driver behavior and a breakdown of car trips taken to data brokers that work with auto insurance carriers. Some people who drive GM-manufactured vehicles saw their insurance premiums skyrocket, yet had no idea why.[69] Our current surveillance economy relies on this lack of self-awareness. Given the decentralized and ubiquitous nature of digital dataveillance, from both private and public entities, protecting data from monitoring is nearly impossible.[70] Those being watched often possess minimal understanding of who is doing the watching or what happens to their PII once it is collected.[71]

The antidote to this "secret, one-way panopticon"[72] must originate with policymakers, who possess the authority and obligation to preserve our democratic institutions. One way officials could foster confidence in government is by developing "trustworthy mechanisms" to ensure PII is collected only when consent has been granted and that data is used responsibly. Our research team agrees with Botsman that transparency is foundational to restoring trust in the system.[73] In fact, this goal of reducing opacity is a catalyst for deploying Long Beach's Digital Rights Platform. While transparency may be accompanied by new complications, it is the "ethical course of action."[74]

The following section explores a relevant central research question: whether the Digital Rights Platform strengthens trust in local government and/or bolsters comfort levels with civic technologies.

Transparency, accountability, and personal empowerment

Data privacy "protections" like terms of service agreements are grounded in the ideals of transparency and accountability. Arguably, though, transparency is wholly insufficient. As opposed to transparency, some scholars assert that the necessary remedy involves severely limiting data collection by smart technologies in the first

[68] Shoshana Zuboff, "Caveat Usor: Surveillance Capitalism as Epistemic Inequality," in *After the Digital Tornado*, ed. Kevin Werbach (Cambridge University Press, 2020), 174–214.

[69] Kashmir Hill, "How G.M. Tricked Millions of Drivers Into Being Spied On (Including Me)," *New York Times*, April 23, 2024, https://www.nytimes.com/2024/04/23/technology/general-motors-spying-driver-data-consent.html.

[70] David Lyon and Zygmunt Bauman, *Liquid Surveillance: A Conversation* (Wiley Publishing, 2013).

[71] Deborah Lupton and Mike Michael, "'Depends on Who's Got the Data': Public Understandings of Personal Digital Dataveillance," *Surveillance & Society* 15, no. 2 (2017): 254–68.

[72] Kevin Kelly, *The Inevitable* (Viking Press, 2016).

[73] Botsman, *Who Can You Trust?*, 175.

[74] Seberger and Shaffer "Rules of Play," 13.

place. As far back as 1989, legal scholar Paul Schwartz predicted that computers would render privacy laws and regulations obsolete and threaten human autonomy: "The more that is known about a person, the easier it is to control him. Insuring the liberty that nourishes democracy requires a structuring of societal use of information and even permitting some concealment of information."[75]

During user testing events, study volunteers frequently agreed with this sentiment. Many reported that the Digital Rights Platform's data privacy notices and online portal, while valuable, fail to go far enough because they cannot opt out of data collection by civic technologies. "One thing that really struck me today is how many amazing city services I'm essentially locked out of if I choose to not sacrifice my privacy. When I go to the airport, I can opt out of facial recognition…Where's my opt-out from the City that gives me an equivalent or similar experience?" a volunteer commented. Another platform tester asserted that Digital Rights Platform data privacy labels "should tell me about opting out or alternatives that are reasonable."

Multiple study participants echoed these concerns, pointing out that there is no alternative when it comes to many activities, from commuting to school on an electric scooter to working on a public computer at the library. Even if people were granted the ability to "consent" to data collection from all civic technologies, scholars challenge the authenticity of consent. "The claim that someone has consented or acted voluntarily may be rebutted with a surprising variety of counterevidence," asserts law professor Don Herzog.[76] As humans, our freedom is predicated on the ability to freely make choices. How autonomous are we, though, when presented with a choice between accepting a complex 5,000-word terms of service agreement, or losing access to a public park dotted with smart streetlamps? The monopoly power exerted by the City's third-party vendors illegitimatizes consent in many contexts. Legal scholar Julie Cohen summarizes it this way: "The issues that users must navigate to understand the significance of consent are too complex and the conditions surrounding consent too easy to manipulate."[77]

While the Digital Rights Platform provides residents with detailed information about how the City collects, uses and stores resident data, study participants reported that reading and scanning privacy notices each time they

---

[75] Paul Schwartz, "The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination," *American Journal of Comparative Law* 37 (1989): 676, DOI:10.2307/840221.

[76] Don Herzog, *Happy Slaves: A Critique of Consent Theory* (University of Chicago Press, 1989), 229.

[77] Julie Cohen, "How (Not) to Write a Privacy Law," Knight First Amendment Institute at Columbia University, March 23, 2021, https://knightcolumbia.org/content/how-not-to-write-a-privacy-law.

encounter City-deployed technologies is unrealistically burdensome. Comments included:

- "It would just be one more thing I'd really not pay attention to, just being honest."
- "You're already so bombarded with cookie permissions and all this other stuff…"
- "I want to get on a bike. I don't really have time to read all that."
- "I'm not going to take the time to scan that QR code."
- "I don't go around scanning QR codes all over the place."

These findings reflect a key characteristic of privacy: while consumers value privacy for privacy's sake, that value is predicated on an individual's own priorities[78]—such as how important it is to know when the bus is arriving in real time, even if one must share travel patterns with a transit app to find out. Further, government dataveillance isn't always obvious; consider the security camera perched high above one's line of sight or the ALPRs mounted on a passing police vehicle. The direct observation and physical inspection Foucault[79] theorizes about when describing the panopticon has been supplanted by far more invasive dataveillance practices. Today, governmental entities and corporations—often working in tandem—carry out surveillance for both private and public purposes.[80] Stated goals run the gamut from ensuring safety to streamlining services to maximizing profits.

Further, modern bureaucracies rely on so-called big data to reduce costs through "efficiencies," to streamline services, and to catalyze innovations. For example, in order to time traffic light intervals that avoid bottlenecks at busy intersections, municipal public works departments analyze data collected through traffic cameras and sensors. These are both screenless technologies with which residents unconsciously (but routinely) interact. It is not an exaggeration to assert that smart city surveillance is nearly ubiquitous—taking place "within public, semi-public and private spaces."[81] Even the lawful driver who is not suspected of violating any traffic rules remains subjected to a license plate scan while entering a city-operated parking garage. Enabled by networked surveillance, this driver's personal information then becomes available to the private company managing that parking garage, to the municipality's public works department, to the credit card company

[78] Joseph Farrell, "Can Privacy Be Just Another Good?" *Journal on Telecommunications and High Technology Law* 10 (2012): 251–64.
[79] Michel Foucault, *Surveiller et Punir: Naissance de la Prison* (Gallimard, 1975).
[80] Galič, "Big Brother," 306–11.
[81] Ibidem, 308.

responsible for processing payments, to the ALPR technology developer and, potentially, to data brokers who aggregate and repackage PII.

In its current iteration, Long Beach's Digital Rights Platform lacks the functionality to prevent scenarios like this one. Even so, some study participants said the Platform bolstered their faith in local government. "I think it's really helpful for the City to provide [data collection] information and to make it accessible to people who want to follow up on it," one volunteer said. Another study participant asserted that informing residents about devices and software in use, and why the City is deploying them, helps "foster acceptance of technology." These comments speak to the notion of epistemic rights, which require society to guarantee that all citizens are given "truthful information and knowledge and the competence to use these for their own benefit and that of society as a whole."[82] Epistemic rights are crucial to both the current policy debate and to critical scholarship on the topic of surveillance technologies. Residents have a right to know how their data is collected and utilized during routine tasks, i.e. when using a TAP card to ride the subway, when checking out a library book, when logging onto a municipal WiFi network—particularly when that usage has the potential to result in discriminatory impacts or other harms. Although local governments rarely adopt surveillance applications for the purposes of monitoring residents or repressing minoritized communities, these outcomes are no less real.

This evokes our study's final central question, which asks whether Long Beach's Digital Rights Platform shifts power from technology companies and local government to residents. Our findings make it clear that transparent data practices enabled by the Platform do not erase power asymmetries created by the use of surveillance technologies. As Richard Whitt writes, asymmetrical computational systems lead to imbalanced information flows and "traditional accountability concepts, like notice and choice, can become meaningless in these environments."[83] Theoretically, data privacy statutes such as the CCPA confer control over personal data to residents. However, the realities of civic technology management—the involvement among multiple actors, sharing and repurposing of data, ubiquitous deployment in public spaces, big data processing—weaken rights granted under the

[82] Hannu Nieminen, "Why We Need Epistemic Rights," in *Epistemic Rights in the Era of Digital Disruption*, ed. Minna Aslama Horowitz, Hannu Nieminen, Katja Lehtisaari, and Allesandra D'Arma (Springer, 2024), 11.

[83] Richard Whitt, "From Thurii to Quayside: Creating Inclusive Digital Communities," *Medium*, Oct. 22, 2020, https://whitt.medium.com/from-thurii-to-quayside-creating-inclusive-digital-communities-348cde93215f.

law. What remains is a "distributed, situated and often microscopic" power relationship.[84]

The following section explains how findings from user testing are informing both changes to the Digital Rights Platform and Long Beach's data privacy policies.

Implications and future research

The findings from our March 2024 user testing events are informing the design of new functionalities for Digital Rights Platform. Specifically, we are collaborating with privacy engineers at Carnegie Mellon University to develop a mobile privacy assistant that makes it simple for residents to set privacy preferences, and to request that third-party actors delete currently held data about them (a right granted under the CCPA). Most significantly, the app would enable residents to opt out of data collection by civic technologies, when feasible. Finally, the privacy assistant we envision would allow residents to configure settings that determine which civic technologies they receive notifications about and how frequently—a functionality informed by previous research concluding that some people would rather not be repeatedly notified about the collection and use of their data, and may even be annoyed by information about some of these practices.[85] As the Digital Rights Platform features evolve and scale, and are adopted by other cities, this project has the potential to grant residents meaningful agency over how they share personal data while interacting with surveillance technologies.

In addition to supporting this future iteration of the Digital Rights Platform, the City of Long Beach is developing a suite of policies meant to advance digital rights. Most consequential is a proposed Data Privacy Policy currently under internal review. When finalized, this document will create a risk-based procedure and minimum threshold for evaluating the privacy impacts of technology systems. The policy will mandate that technology systems posing a "medium" or "high" risk to data privacy be subject to a privacy impact assessment. Finally, that technology's use policy will be added to the Digital Rights Platform registry of civic technologies that collect PII.

---

[84] Ilia Antenucci, "Smart Cities, Smart Borders: Sensing Networks and Security in the Urban Space," in *Sensing In/Security: Sensors as Transnational Security Infrastructures*, ed. N. Klimburg-Witjes, N. Poechhacker and G. Bowker (Mattering Press, 2020), 48.

[85] Acquisti, Alessandro, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, Yang Wang, and Shomir Wilson, "Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online," *ACM Computing Surveys* 50, no. 3 (2017): Article 44.

Conclusion: Granting agency over personal information is a complex but achievable goal

Our research findings underscore that public engagement and education about a technology's intended purpose, functions and benefits are vital to instilling trust.[86] For example, one study participant pointed out the risks of opaqueness surrounding municipal data collection: "The problem right now is that people don't trust the City. So as long as you keep things away from people, it's going to be tough." Others went further, with one participant asserting that the City has a "legal responsibility" to let residents know when they are "being screened, recorded, or having their pictures taken." When policymakers neglect to articulate the positive aspects of even benign smart city projects, members of the public are left to speculate—and to draw conclusions that sometimes clash with reality and, perhaps, unnecessarily foster distrust. Conversely, when civic technologies infringe upon residents' privacy, local government should be held accountable. Data collected during user testing events show that the Digital Rights Platform has a vital role to play in both these scenarios.

As discussed throughout this article, simply moving through one's day means interacting with sensors, cameras and kiosks in public spaces. As a society, we've come to accept that our images are captured, our movements recorded and our digital transactions analyzed because no real opt-out exists. Multiple factors contribute to users' lack of control, such as screenless systems and applications running "in the background." Various potential remedies have been proposed. For example, an "architectural control" policy would mandate that smart cities and their vendors adopt "full transparency" regarding how they process data; that they limit data processing to specific purposes; and that they implement technical measures to prevent data breaches.[87] An alternative fix would be to flip the current "opt out" by default scheme to a design where users "opt in" to data collection by default. The most comprehensive potential solution, a federal privacy law strictly limiting the types of PII private and public entities may collect to begin with, is also the most contested. In the absence of remedies such as these, Long Beach's Digital Rights Platform offers a meaningful attempt to shrink power asymmetries between residents and civic technologies.

---

[86] Kirsten Heidelberg, "Trust in Smart City Systems: Characteristics and Key Considerations," January 2020. Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/sites/default/files/publications/Trust%2520in%2520Smart%2520City%2520Systems%2520Report%252020200715_508.pdf.

[87] Athena Christofi and Valerie Verdoodt, "Exploring the Essence of the Right to Data Protection and Smart Cities," KU Leuven Centre for IT and IP Law: 6, https://ssrn.com/abstract=3483616.

This research was supported by the National Science Foundation [award number 2234081].

Bibliography

Acquisti, Alessandro, Curtis Taylor, and Liad Wagman. 2016. "The Economics of Privacy." *Journal of Economic Literature* 54, no. 2: 442–92. http://doi.org/10.1257/jel.54.2.442.

Allen, Anita, "Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm." *Connecticut Law Review*. All Faculty Scholarship (2000). https://scholarship.law.upenn.edu/faculty_scholarship/790.

Allen, Anita. "Dismantling the 'Black Opticon': Privacy, Race, Equity and Online Data-Protection Reform." *The Yale Law Journal* 131 (2021).

Antenucci, Ilia. "Smart Cities, Smart Borders: Sensing Networks and Security in the Urban Space." In *Sensing In/Security: Sensors as Transnational Security Infrastructures*, edited by Nina Klimburg-Witjes, Nikolaus Poechhacker and Geoffrey Bowker, 46-64. Mattering Press, 2020.

Apple. "Set Up Voice Recognition and Personal Requests," accessed July 13, 2024. https://support.apple.com/en-ph/guide/homepod/apd1841a8f81/homepod.

Arrow, Kenneth. "The Economics of Information: An Exposition." *Empirica* 23 (1996): 119–28.

Asid, Asid. *Engage and Evade: How Latino Immigrant Families Manage Surveillance in Everyday Life*. Princeton University Press, 2023.

Barsa, Michael. "California's Proposition 65 and the Limits of Information Economics." *Stanford Law Review* 49, no. 5 (1997): 1223–47.

Braun, Matthias, and Patrik Hummel. "Is digital sovereignty normatively desirable?" *Information, Communication & Society* (2024): 1–14. https://doi.org/10.1080/1369118X.2024.2332624.

Burchell, Graham, Colin Gordon, and Peter Miller. *The Foucault Effect: Studies in Governmentality*. University of Chicago Press, 1991.

Cagle, Matt. "Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color. ACLU of Northern California." October 11, 2016. https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target.

California Office of Environmental Health Hazard Assessment. "Proposition 65," accessed July 13, 2024. https://oehha.ca.gov/proposition-65.

Chawdhry, Adnan, Karen Paullet, and Jamie Pinchot. "Internet of Things: Measuring Data Privacy Concerns of Users." *Issues in Information Systems* 23, no. 4 (2022): 94–110. https://doi.org/10.48009/4_iis_2022_109.

Chakraborty, Aindrila, Ramesh Shankar, and James Marsden. "An Empirical Analysis of Consumer-unfriendly E-commerce Terms of Service Agreements: Implications for Customer Satisfaction and Business Survival." *Electronic Commerce Research and Applications* 53 (2022): 101151. https://doi.org/10.1016/j.elerap.2022.101151.

Christofi, Athena, and Valerie Verdoodt. "Exploring the Essence of the Right to Data Protection and Smart Cities." KU Leuven Centre for IT and IP Law, 2019. https://ssrn.com/abstract=3483616.

City of Long Beach. "Framework for Racial Reconciliation," effective June 26, 2020. https://longbeach.legistar.com/View.ashx?M=F&ID=8595273&GUID=107D5EFA-D10F-4444-B35A-3E7C272887BD.

City of Long Beach. "Data Privacy Guidelines," effective March 2021,

http://longbeach.gov/globalassets/smart-city/media-library/documents/final_data-privacy-guidelines.

Cottrill, Caitlin, Naomi Jacobs, Milan Markovic, and Pete Edwards. "Sensing the City: Designing for Privacy and Trust in the Internet of Things." *Sustainable Cities and Society* 63 (2020): Article 102453. https://doi.org/10.1016/j.scs.2020.102453.

Crespi, Francesco, Serenella Caravella, Mirko Menghini, and Chiara Salvatori. "European Technological Sovereignty: An Emerging Framework for Policy Strategy," *Intereconomics* 56, no. 6 (2021): 348–54. https://doi.org/10.1007/s10272- 021-1013-6.

Data USA. "Long Beach, CA. Population and Diversity," accessed July 15, 2024. https://datausa.io/profile/geo/longbeach-ca.

Emejulu, Akwugo, and Callum McGregor. "Towards a Radical Digital Citizenship in Digital Education." *Critical Studies in Education* 60, no. 1 (2019): 131–47. https://doi.org/10.1080/17508487.2016.1234494.

Esposti, Sara Degli. "When Big Data Meets Dataveillance: The Hidden Side of Analytics." *Surveillance & Society* 12, no. 2 (2014): 209–25.

Federal Bureau of Investigation. “Ransom Attacks Straining Local U.S. Governments and Public Services.” March 30, 2022. https://www.ic3.gov/Media/News/2022/220330.pdf.

Flores, Kevin. "City Council to Decide Whether to Buy Controversial License Plate Readers." *Forthe*, November 17, 2020. https://forthe.org/journalism/license-plate-readers/.

Foucault, Michel. *Surveiller et Punir: Naissance de la Prison.* Gallimard, 1975.

Galič, Maša. “Smart Cities as ‘Big Brother Only to the Masses’: The Limits of Personal Privacy and Personal Surveillance.” *Surveillance & Society* 20, no. 3 (2022): 306–11. https://ojs.library.queensu.ca/index.php/surveillance-and-society/index.

Glaser, Barney, and Amselm Strauss. *The Discovery of Grounded Theory: Strategies for Qualitative Research*, 2nd ed.,Transaction Publishers, 1999.

Hardin, Russell. *Trust*. Polity Press, 2006.

Heidelberg, Kirsten. *Trust in Smart City Systems: Characteristics and Key Considerations*.

Cybersecurity & Infrastructure Security Agency, January 2020. https://www.cisa.gov/sites/default/files/publications/Trust%2520in%2520Smart%2520City%2520Systems%2520Report%252020200715_508.pdf.

Helpful Places. “2022 DTPR City Cohort Program Report,” 2022.

Herzog, Don. *Happy Slaves: A Critique of Consent Theory*. University of Chicago Press, 1989.

Hill, Kashmir. “How G.M. Tricked Millions of Drivers Into Being Spied On (Including Me).” *New York Times*, April 23, 2024. https://www.nytimes.com/2024/04/23/technology/general-motors-spying-driver-data-consent.html.

Hiter, Shelby. “AI and Privacy Issues: Challenges, Solutions, and Best Practices.” eWeek. Accessed July 13, 2024. https://www.eweek.com/artificial-intelligence/ai-privacy-issues/.

Jotto. “Want Real Insights from Your Community?” accessed August 1, 2024. https://www.jotto.video/.

Julsrud, Tom and Krogstad, Julie. “Is There Enough Trust for the Smart City? Exploring Acceptance for the Use of Mobile Phone Data in Oslo and Tallinn.” *Technological Forecasting and Social Change* (2020): 120314. https://doi.org/10.1016/j.techfore.2020.120314.

Kelley, Patrick G., Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder. "A 'Nutrition Label' for Privacy." In Symposium on Usable Privacy and Security (SOUPS) Proceedings. Mountain View: 2009.

Kitchin, Rob. *Getting Smarter About Smart Cities: Improving Data Privacy and Data Security*. Data Protection Unit, Department of the Taoiseach, Dublin, Ireland, 2016.

Lupton, Deborah and Mike Michael. "'Depends on Who's Got the Data': Public Understandings of Personal Digital Dataveillance." *Surveillance & Society* 15, no. 2 (2017): 254–268. doi.org/10.24908/ss.v15i2.6332.

Lyon, David, and Zygmunt Bauman. *Liquid Surveillance: A Conversation.* Wiley, 2013.

McDonald, Nora, and Andrea Forte. "The Politics of Privacy Theories: Moving from Norms to Vulnerabilities." In CHI '20 Proceedings, 1–14. Honolulu: 2020.

Medina, Mekahlo. "City Confirms Data Was Stolen in Cyberattack," *NBC Los Angeles*, November 29, 2023. https://www.nbclosangeles.com/local-2/city-of-long-beach-confirms-data-was-stolen-in-cyberattack/3279847/.

National Institute of Standards and Technology. *NIST Privacy Framework*, January 16, 2020. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf.

Nieminen, Hannu. "Why We Need Epistemic Rights." In *Epistemic Rights in the Era of Digital Disruption*, edited by Minna Aslama Horowitz, Hannu Nieminen, Katja Lehtisaari, and Allesandra D'Arma. Palgrave Macmillan, 2024. doi.org/10.1007/978-3-031-45976-4_2.

Nissenbaum, Helen. "Privacy as Contextual Integrity." *Washington Law Review* 79, no. 1 (2004): 119–57. https://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf.

Nissenbaum, Helen. "Contextual Integrity Up and Down the Data Food Chain," *Theoretical Inquiries in Law* 20, no. 1 (2019): 221–56.

Passport Inc. "Passport Unveils New Performance Benchmarking Solution," June 12, 2023. https://www.passportinc.com/blog/passport-unveils-new-performance-benchmarking-solution/.

Pew Research Center. "Key Findings About Americans and Data Privacy." Last modified October 18, 2023. https://www.pewresearch.org/short-reads/2023/10/18/key-findings-about-americans-and-data-privacy/.

Powell, Allison. "Data Walks and the Production of Radical Bottom-up Data Knowledge." Paper presented at the International Communications Association conference. San Diego, California, May 24, 2017.

Rule, James. “Contextual Integrity and Its Discontents: A Critique of Helen Nissenbaum’s

Normative Arguments.” *Policy & Internet* 11, no. 3 (2019): 260–79. https://onlinelibrary.wiley.com/doi/10.1002/poi3.215.

Salter, Chris. *Sensing Machines: How Sensors Shape Our Everyday Life*. The MIT Press, 2022.

Schneier, Bruce. “How We Sold Our Souls–and More–to the Internet Giants.” *The Guardian*, May 17, 2015. https://www.theguardian.com/technology/2015/may/17/sold-our-souls-and-more-to-internet-giants-privacy-surveillance-bruce-schneier.

Schwartz, Paul. “Internet Privacy and the State.” *Connecticut Law Review* 32 (2000): 815.

Schwartz, Paul. “The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination,” *American Journal of Comparative Law* 37 (1989). https:// DOI:10.2307/840221.

Seberger, John, and Gwen Shaffer. “Changing the Rules of Play in Long Beach, California: Smart Cities, Infrastructure and the Well-Played Game.” *International Journal of Human-Computer Interaction* (2021): 1–16. https://doi.org/10.1080/10447318.2021.2012380.

Shaffer, Gwen. “Applying a Contextual Integrity Framework to Privacy Policies for Smart Technologies.” *Journal of Information Policy* 11 (2021): 222–65. https://www.jstor.org/stable/10.5325/jinfopoli.11.2021.0222.

Solove, Daniel. “The Limitations of Privacy Rights.” *Notre Dame Law Review* 98 (2023): 975.

Statistical Atlas. “Race and Ethnicity in Downtown Long Beach, Calif,” accessed July 13, 2024. https://statisticalatlas.com/neighborhood/California/Long-Beach/Downtown/Race-and-Ethnicity.

Susser, Daniel. “Why privacy disclosures are valuable even if consent frameworks are not.” *Journal of Information Policy*, 9 (2019): 148–73.

Suthivarakom, Ganda. “Wirecutter: What is Prop 65? And Why Is There a Warning Label on This Thing I Bought?” *New York Times*, March 10, 2020. https://www.nytimes.com/wirecutter/blog/what-is-prop-65/.

U.S. Census Bureau. “Long Beach, Calif,” Accessed July 13, 2024. https://www.census.gov/quickfacts/fact/table/longbeachcitycalifornia/PST045222.

U.S. Ignite. “Fostering Civic Trust: A Policy Guide for Municipal Leaders.” May 2021. https://www.us-ignite.org/wp-content/uploads/2021/06/USIgnite-CIVIC-Trust-Guide-Final.pdf.

United Nations. “Universal Declaration of Human Rights.” Effective December 10, 1948. https://www.un.org/en/about-us/universal-declaration-of-human-rights.

Van Dijck, Jose. “Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology.” *Surveillance & Society* 12, no. 2 (2014): 197–208.

Van Es, Karin and de Lange, Michiel. “Data With its Boots on the Ground: Data Walking as a Research Method.” *European Journal of Communication* 35, no. 3 (2020): 278–89. https://doi.org/10.1177/0267323120922.

van Zoonen, Liesbet, Fadi Hirzalla, Jiska Engelbert, Linda Zuijderwijk, and Luuk Schokker. “Seeing More Than You Think: A ‘Data Walk’ in the Smart City.” In *Public Engagement with the Smart City*, edited by S. Hussey, 16-19. Bang the Table, 2017.

Whitt, Richard. *Reweaving the Web*. Glianet, 2024.

Whitt, Richard. “From Thurii to Quayside: Creating Inclusive Digital Communities,” *Medium*, October 22, 2020. https://whitt.medium.com/from-thurii-to-quayside-creating-inclusive-digital-communities-348cde93215f.

Whole Foods. “Easy Ways to Shop and Pay in Stores.” Accessed July 13, 2024. https://www.wholefoodsmarket.com/amazon/payments-and-ways-to-shop.

Zuboff, Shoshana. “Caveat Usor: Surveillance Capitalism as Epistemic Inequality.” In *After the Digital Tornado*, edited by Kevin Werbach, 174-214. Cambridge University Press, 2020. https://doi.org/10.1017/9781108610018.

Zucker, Lynne. “Production of Trust: Institutional Sources of Economic Structure, 1840-1920.” In *Research in Organizational Behavior*, edited by B. Staw and L. Cummings, 53-111. vol. 8: JAI Press, 1986.