Invasive Yet Inevitable? Privacy Normalization Trends in Biometric Technology

Sejin Paik, Kate K. Mays, and James E. Katz

Abstract

As biometric technology relies on bodily, physical information, it is among the more intrusive technologies in the contemporary consumer market. Consumer products containing biometric technology are becoming more popular and normalized, yet little is known about public perceptions concerning its privacy implications, especially from the perspective of human agency. This study examines how people perceive biometric technologies in different societal contexts and via different agents in control. Our study revealed that, in large part, people’s perceptions of biometric technology are context-dependent, based on who retrieves and who benefits from the information and the situation where the data are collected. Participants were much more comfortable with more intrusive biometric technology in airport security than in a grocery store, and if it was employed to improve their health. We conclude by considering the implications of the survey for new threats to personal privacy that arise out of emerging technologies.

Keywords

biometric, facial recognition, DNA identification, digital privacy, digital data sharing, emerging technology, surveillance technology, contextual integrity, situational privacy
wider. This study aims to explore facets of a specific emerging technology—biometrics, as it relates to newfound patterns of public surveillance and methods for collecting networked data.

Biometrics is a technology that falls under these recent trends of persuasive and overt surveillance techniques. The definition of biometrics is the automated authentication of an individual based on his or her unique physical and physiological characteristics that can be measured, recorded, quantified and stored in its digital representation (Bolle, 2004; Elgarah & Falaleeva, 2005). As the definition covers, the primary functions of biometrics are security and identification through the use of bodily data—which can be argued as an even more explicit, sensitive, and intrusive technology. Some of the widely used biometric technologies are facial and eye recognition, DNA matching, voice identification and gesture (hand/body movement) recognition.

Increasingly, everyday people are using biometrics technology in their daily lives and are slowly starting to become more accustomed to providing data to these devices which operate on highly personal, invasive bodily information. Thus, this study expands on a specific branch of privacy and technology literature concentrating on situational (Masur, 2018) and contextual factors (Nissenbaum, 2010). In particular, we investigate (1) how people’s comfort level toward various biometric technologies differ in certain contexts, (2) which agents of control affect individuals’ willingness to share personal data, and (3) how individual traits influence perception of biometric technologies. We end by discussing the privacy concern and technology acceptance level trade-offs that appear with certain combinations of context and agents of control in biometric technologies.

**Literature Review**

**Biometrics: An Emerging Technology**

Technological advancements have allowed for personal computing devices to be available to the general public, and social media as well as online services have made widespread information sharing across these devices a reality. However, many of these personalized and persuasive consumer technologies have subtle, yet consequential power to change individuals’ behaviors, attitudes, and daily habits by making a desired outcome of an individual easier to achieve (Fogg, 2003). These trends in the growing reliance on social media and greater usages of physically intrusive technologies have opened the door to new surveillance opportunities. One major ethical concern attached to these technologies is overt surveillance. The notion of overt surveillance technology creates a power structure similar to Bentham’s panopticon for control (Slobogin, 2003). People’s acceptance of persuasive technologies has been related to multiple factors ranging from involvement, informativeness, usability, social support, credibility, and inspiration (Alhammad & Gulliver, 2014). Biometrics, as a type of surveillance identification technology, is unique in that it depends on human physical characteristics to operate and with that type of data, the system is able to create a multiplying effect on the existing, robust networked (Agre, 1994; Kim, 2004) and personalized technological system.

As biometric technologies are not only used for law enforcement and identification purposes but also increasingly adopted in commercial and civil spaces, scholars of emerging technology ethics emphasize the need for research to realistically capture the complexities of privacy perception and information flow trends occurring with technologies such as biometrics. North-Samardzic (2019) work on applied biometrics and business ethics demonstrates that contextual factors are necessary, yet underutilized measurements to fully capture the privacy dynamics among the users, the agents deploying the technology and the technology itself. Efforts to uncover greater specificity and granularity around an individual’s privacy concerns and intended behavior with a certain technology can protect the rights and civil liberties of those using biometric technologies.

**Situational and Contextual Privacy**

Privacy is one of the most enduring issues in our society. The concept of privacy has been interpreted in different ways throughout history: as a legal right (Warren & Brandeis, 1890), a commodity (Bennett, 1995), or a state (Westin, 1967). Westin (1967) conceptualized privacy as a way for individuals to distinguish and limit access and resources to themselves from others. From a legal definition, privacy is the right to control circulation of information about oneself or to have a right to erasure of information (General Data Protection Regulation, 2020). With the current technological systems, a state of complete anonymity or reserve is hard to achieve, due to the wide array of commercialized and publicly available channels that are used to spread personal information. In the space of online advertising, “digital identities” of consumers are created not only for information storage, but also to generate inferential and predictive profiling measures (Mathews-Hunt, 2016). Subsequently, individuals have less control over their information share and spread due to the networked power of current social media and surveillance technologies.

Theories such as the privacy paradox and privacy calculus have been widely adopted to understand how people perceive and approach privacy issues when it comes to technology use. Privacy calculus is based on risk–benefit analysis (Dinev & Hart, 2006), while the privacy paradox is used to observe an individual’s stated privacy beliefs and their actual actions toward a given technology (Barnes, 2006). Literature shows that people tend to disclose personal information when the technology provides convenience and efficiency to one’s lifestyle (Taddicken, 2013).

Extending beyond the general factors that play into privacy perceptions on emerging technology use, this study considers
a multifaceted approach to understanding people’s willingness to share private information through a given technology. Burgoon (1982) was one of the earliest scholars to introduce the idea that conceptualization around privacy is subjective and situational in nature. The author suggested four interrelated dimensions of privacy: physical, interactional, psychological, and informational access. These four dimensions play a large role in shaping an individual’s interpretation of privacy given one’s situation and personal experience.

A contemporary take on Burgoon’s work is Masur’s (2018) theory on situational privacy that explores how interpersonal, environmental, and situational factors affect levels of online privacy literacy and people’s actions to self-disclosure. Masur’s theory is multidimensional and processual in nature, where he builds on existing privacy values such as awareness of economic practice, technical skills (Hoofnagle et al., 2010), and factual knowledge (Trepte et al., 2015), and combines these with other dimensions such as horizontal (i.e., interpersonal and personal privacy perceptions) and vertical (i.e., types of agents involved such as commercial vs public institutions) (Masur, 2020). He also ran an empirical study to measure perceptions of environmental factors in relation to people’s usage of smartphones and found that people are more inclined to disclose private information in settings where levels of privacy protection was higher (Masur, 2018). The perception of higher levels of privacy was defined by characteristics such as trustworthiness and similarities in interests, needs, and values pertaining to psychological and environmental factors.

Building on the idea that privacy perception is situational, we lay the groundwork for our study using contextual integrity (Nissenbaum, 2010), a socio-legal theory that identifies the impact of context-relative norms when it comes to individuals’ decisions to participate or forgo information sharing practices. For Nissenbaum, privacy is defined as “neither a right to secrecy nor a right to control but a right to appropriate flow of personal information” (Nissenbaum, 2010, p. 127). Her theory assumes that privacy and technology norms are created through a concert of various power players such as family, religion, political belief, history, culture, and corporations. Nissenbaum’s conceptualization of context relies on: (1) the differentiation between public and private contexts and (2) social institutional spheres such as education, health care, religion, consumer activity, and interpersonal relationships. The work relies on the idea that different informational privacy expectations are governed in different social settings. Under the contextual framework, privacy threat occurs when the norms, values, and social practices of informational sharing in the expected social contexts are violated or misaligned.

In recent years, a handful of empirical and critical studies have applied contextual integrity to specific technologies and social contexts. Apthorpe et al. (2018) created a contextual integrity survey method to discover privacy norms in the realm of smart home devices. The results showed only one parameter (out of five) with a positive pairwise acceptability score: “if its owner has given consent” (Apthorpe et al., 2018). Conversely, parameters with the lowest acceptability score were when information would be distributed for advertisements and information storage was indefinite. Extending on Apthorpe et al.’s (2018) findings are North-Samardzic’s (2019) discussions on the ethical implications of biometric technology applications. North-Samardzic (2019) emphasized the need for preventive awareness on the technical capabilities of second-generation biometrics, as these technologies will easily be employable without informed consent.

Norval and Prasopoulou’s (2017) critical analysis is another example of the use of Nissenbaum’s framework to understand people’s perception of facial recognition technology. They argue that the framing of emerging technologies such as biometrics are “not neutral” and the discourses around these technologies are constantly reworked, a process they define as contexts of iteration. Given this practice, the authors propose that the diffusion of a technology’s perception does not carry over seamlessly from one context to another. Contributing to this body of growing literature on situational and contextual privacy in the space of biometric technology, our study examines the perception of two biometric technologies—facial recognition and DNA identification technology—given individual traits and external, context, and situation-based variables.

**Contextual Factors in Willingness to use Biometric Technology**

The context in which biometric technology is openly adopted, used, and accessed occurs in multiple societal dimensions. At an individual, consumer level, biometric technology became ubiquitous in mobile phones and laptops through the introduction of the touch ID in 2014, which replaced the action of typing and remembering passwords and payment information (Phillip Redman, 2015). In 2017, the touch ID evolved to the commercialization of facial recognition technology. Mobile phone consumers transitioned through different authentication systems over the span of 10 years, from manually typing in their passcodes, using the touch ID function, to flashing their faces on mobile screens to unlock their devices. Simultaneously, these changes took place in the world of online banking and shopping. Biometrics for online payment authentication grew, both for security and convenience purposes. In January 2020, a Visa corporation–led consumer survey report showed that two-thirds of online shoppers preferred to use fingerprint or facial recognition features over the use of traditional passwords (AYTM Market Research, 2017).

At a societal level, biometrics is used in the fields of health care, transportation and law enforcement. One example of biometrics technology implemented in the public space that tackles both individual and national security measures are at airports around the world. In the United States,
the Transportation Security Administration (n.d.) began using facial recognition and fingerprint systems to identify passengers in 2015. From 2018, over 20 US airports have launched the use of facial recognition technology for passengers entering and exiting the country. Similar to the reasons used for enhancing personal device authentication procedures, the use of biometrics in airports has been promoted on the basis of efficiency—both in terms of speeding up the verification process and decreasing the chances for manual errors. However, the use of biometrics in airports have increased discussions around the concern that the technology will lead to a comprehensive tracking system, which would contain highly sensitive data with major repercussions if leaked or hacked (J. Davis, 2019).

As the examples above show, people have slowly been led to have no choice but to incorporate and accept biometric technologies both at an individual, convenience level and at a societal, public security-level. While individuals express that they are wary, anxious, and alarmed at the potential risks of losing control of their privacy in this digital era (Molla, 2019), there is no decline in the sales and uses of devices containing the biometric technology, particularly as the factors of convenience, usefulness, and enjoyment are overridden when met with the question of privacy concerns.

We distinguish the two concepts: “context” and “situation,” used in this study. When we operationalize “context,” we refer to Nissenbaum’s conceptualization of context as structured social settings relating to domains such as family, travel, health care, and physical and digital consumer product spaces. We then adapted a subsection of Masur’s situational privacy which pertains to the external environmental norms commonly followed by a given social setting to create realistic, hypothetical situations that we could measure within the broader contexts.

Our study considers four contexts—grocery store, airline security, home security, and public safety. Grocery stores and airlines fall under Nissenbaum’s consumer category. Home security falls into a combination of family setting, consumer context, and a form of self-surveillance. Finally, public safety falls under the policing and public surveillance context, which is different from social contexts. With these specific contexts, we propose our first research question:

**RQ1.** Given certain contexts, how does people’s comfort level toward two biometric technologies: DNA identification and facial biometric technologies, differ?

**Agents of Control**

**Public versus Private Entities.** Two major agencies overtake the implementation of biometric technologies: the government (public) and the corporate (private). While both parties execute the technology for the same security or identification purpose, the way they communicate the usefulness and need for the technology’s integration into society vary.

Social versus Institutional. Another aspect to consider is the difference in perception between social and institutional agents in control. Social privacy refers to other users’ accessing one’s private data and institutional privacy relates to how third-party companies use people’s private data (Young & Quan-Haase, 2013). Studies that measure the impact of these two conceptual groupings are split in results. Young and Quan-Haase’s (2013) work showed that their participants were overwhelmingly more concerned with their social...
privacy than they are with institutional privacy. According to a Pew Research Center survey, 56% of the American population trust law enforcement to use facial recognition responsibly, compared with the 36% trust to technology companies and 18% trust to advertisers (Smith, 2020). Along the same lines, a different Pew Research Center survey found that 81% of the public think that the potential risks of personal data collection by companies are much greater than the benefits, with 66% answering the same about government data collection (Auxier et al., 2019).

However, Lutz and Newlands (2021) measured privacy concerns around the usage of smart speakers and their survey results showed that users reported higher concerns around institutional privacy, such as concerns about contractors and third-party developers accessing personal data over those in the category of social privacy such as other household members. Adding to Lutz & Newlands’ work, a qualitative study that observed privacy attitudes on various technologies such as Ring surveillance cameras, a parking app and internet-connected water meters showed that residents noted higher concerns and mistrust for their public officials and local government agencies collecting personal information through these devices (Shaffer, 2020). Respondents of the Shaffer (2020) study vocalized overwhelming opposition to the practice of local governments collecting and selling it to third-party service providers.

Even with these varying scenarios of mistrust and concern, people continue to use these highly interconnected, intrusive technologies in their personal homes or in public settings. These discrepancies in previous findings motivate us to investigate the impact of public versus private agents in affecting the different levels of individual’s attitudes and comfort levels toward a particular type of technology and its privacy capabilities.

**RQ2.** How do the types of agents in control affect people’s response to the use and sharing of data via biometric technology?

**RQ3.** How do individuals’ privacy concerns and concerns for information misuse affect the way people conceive of two biometric technologies: DNA identification and facial recognition?

### Methods

#### Study Design and Sample

A survey was conducted (April–May 2021) through an online questionnaire administered by Qualtrics, a US-based international company that partners with over 20 online panels to provide diverse and quality participants. Participants were paid by Qualtrics, though the specific amount each participant received was unknown. The questionnaire included several attention and quality checks to ensure responses were valid and reliable. Qualtrics removed participants who finished the survey too quickly (in half the median complete time) or who appeared to be “straightliners,” meaning that they provided the same answer to all questions. Quotas were established for gender, age, race, income, and education based on demographic distributions in the United States to recruit a nationally representative sample (N=1,150). Accordingly, our sample was 54.1% female, average age was 50.10 years old, 62.2% White/Caucasian, 64.3% made less than US$75,000 on household income, and 54.6% had less than a Bachelor’s degree. (Refer to Table 1 for a full breakdown of demographic descriptive statistics.)

### Measurement

Participants were asked a series of questions to measure their attitudes about surveillance and privacy technology that utilize a range of emerging biometrics, as well as measures to capture individual traits (Table 2).

---

**Table 1.** Descriptive Statistics of Demographic Variables.

| Variables                  | M (SD) | %          |
|----------------------------|--------|------------|
| Gender                     |        |            |
| Male                       | 45.5   |            |
| Female                     | 54.1   |            |
| Age (18–79 years)          | 50.10 (18.18) |        |
| Household income           |        |            |
| Less than US$25,000        | 22.2   |            |
| US$25,000–49,999           | 26.2   |            |
| US$50,000–74,999           | 15.8   |            |
| US$75,000–99,999           | 11.0   |            |
| US$100,000–149,999         | 11.7   |            |
| US$150,000 or more         | 7.7    |            |
| Education                  |        |            |
| Less than high school diploma | 1.8 |          |
| High school diploma        | 20.2   |            |
| Some college (no degree)   | 21.7   |            |
| Associate’s degree          | 10.8   |            |
| Bachelor’s degree           | 29.2   |            |
| Graduate degree             | 15.2   |            |
| Race/ethnicity             |        |            |
| White/Caucasian            | 62.2   |            |
| Black/African American     | 14.2   |            |
| Hispanic/Latino            | 13.0   |            |
| Asian-American             | 6.2    |            |
| Others                     | 3.5    |            |
| Political Ideology         |        |            |
| Progressive                | 8.8    |            |
| Liberal                    | 31.1   |            |
| Conservative               | 27.9   |            |
| Very conservative          | 10.3   |            |
| Libertarian                | 3.3    |            |
| Others                     | 6.9    |            |

Note. “Choose not to respond” items were not included, which may explain for some variables not adding up to 100%. SD = standard deviation.
sphericity was significant, the measure of sampling adequacy was 0.92, and Bartlett’s test of sphericity was significant. The Kaiser–Meyer–Olkin (KMO) measure of sampling adequacy was 0.93, and Bartlett’s test of sphericity exceeded the critical chi-square value = 5.92) explained 59.17% of the variance and consisted of five items (see Table 3) related more to others—private pharmaceutical companies, researchers, and law enforcement—benefiting from the data-sharing (M=3.36, SD=2.61, α=.92). The second factor (eigenvalue = 1.55) explained an additional 15.48% of the variance; these items related to individual benefit of data-sharing, such as learning more about one’s genealogy, connecting to relatives, and determining health risks like cancer (M=5.16, SD=2.50, α=.91).

Facial Recognition. The scale for comfort with facial recognition technology included 10 items, and similar to the DNA items, varied on who would receive and benefit from the data sharing (Table 4). They included statements that asked how comfortable one would feel if a surveillance camera: “uses facial recognition to match your face against a list of employees in your workplace, helping security spot unknown people,” “lets police departments scan crowds in real time, looking for known criminals,” and “tracks where you look in a store (but not who you are) to see which products catch your attention.”

The factorability of comfort with facial recognition technology was deemed appropriate: All items correlated with one another above 0.30, the Kaiser–Meyer–Olkin (KMO) measure of sampling adequacy was 0.93, and Bartlett’s test of sphericity was significant (χ²(55)=14,170.70, p<.001. The EFA revealed that one factor (eigenvalue=7.98) explaining 72.55% of the variance could be extracted to comprised the facial recognition comfort construct (M=5.55, SD=2.63, α=.94).

**Table 2. Descriptive Statistics of Key Measures.**

| Measures (scale)               | M (SD)     | Cronbach’s α |
|-------------------------------|------------|--------------|
| Misuse of information (1–4)   | 2.86 (.73) | .88          |
| Privacy concern (1–5)         | 4.16 (.81) | .93          |
| Support for gpy. surveIlance (1–5) | 3.53 (.91) | .91          |
| Locus of control (1–5)        | 2.50 (.67) | .77          |
| Perceived tech competence (1–5) | 3.36 (.84) | .87          |

**Note. SD = standard deviation.**

**Perceptions of Privacy-Invasive Technology.** Two scales were developed from *The New York Times*’ interactive feature entitled “Where would you draw the line?” (Thompson et al., 2019). In this piece, readers were presented with different “scenarios at the intersection of privacy and technology” that progressed with increasing invasions of personal privacy and asked to move a virtual line and stop at the scenario that represented the limit of their comfort. From these scenarios, two scales measuring respondents’ comfort with (1) DNA identification and (2) facial recognition were created and evaluated using an exploratory factor analysis (EFA). Respondents were asked to indicate how comfortable they were with DNA identification and facial recognition technology being used in the scenarios put forth by *The New York Times* on a 10-point slider scale (very uncomfortable–very comfortable). The scale for comfort with DNA biometric technology included 10 items that varied in terms of who the recipient and beneficiary of one’s data are. They included statements that asked how comfortable one would feel if a DNA company, “uses your DNA sample to offer clues about your genealogy,” “sells an analysis of your anonymous DNA profile to pharmaceutical companies,” and “lets law enforcement agencies register as users, which lets them look for criminals by matching DNA profiles (without a warrant).”

The factorability of comfort with DNA identification technology was deemed appropriate: All items correlated with one another above 0.30, the Kaiser–Meyer–Olkin (KMO) measure of sampling adequacy was 0.92, and Bartlett’s test of sphericity was significant (χ²(45)=8,869.30, p<.001. The EFA revealed two factors could be extracted, explaining 74.65% of the total variance. The first factor (eigenvalue=5.92) explained 59.17% of the variance and consisted of five items, varied on who would receive and benefit from the data-sharing (M=3.36, SD=2.61, α=.92). The second factor (eigenvalue=1.55) explained an additional 15.48% of the variance; these items related to...
Surveillance Contexts. There were four different real-life contexts we put forth, in which people typically give up information about themselves: grocery store, airline security, home security, and public safety. We kept the context and agent of control constant and varied the technology within each domain. Given these context-situations’ unique circumstances, the types of technologies varied somewhat to remain context-sensitive and realistic. Accordingly, the type of measurement was determined individually for each context and was not consistent across all four scenarios.

Grocery Store. For questionnaires pertaining to grocery stores, we asked participants about different scenarios where technology would be integrated into their grocery shopping experience. Based on a 5-point Likert-type scale with five items, participants were asked how comfortable they would be in use-cases such as in-store cameras built in the grocery store to thwart shoplifters and in-store cameras that log one’s shopping activity for personalized product recommendations.

Home Security. To gauge perceptions of various technologies with a private company as an agent of control, participants were asked what they thought of a home security company offering a variety of new products under consideration.

| Table 4. Comfort With Facial Recognition Technology—Exploratory Factor Analysis. |
|---------------------------------------------------------------|
| Items                                                      |
| uses facial recognition to match your face against a list of employees in your workplace. |
| checks your face against a database of tenants in your apartment building. |
| checks your face against a database of known shoplifters, allowing store security. |
| allows police departments to match your face against a mugshot database to help in an investigation. |
| allows police departments to match your face against a driver’s license database to help in an investigation. |
| monitors major roads or bridges 24/7 by matching drivers’ faces against others. |
| lets police departments scan crowds in real time for suspicious activities. |
| uses facial analysis to determine your age and gender (but not who you are) when buying something in a store. |
| tracks where you look in a store (but not who you are) to see which products catch your attention. |
| interprets the features on your face to guess other attributes about you (but not who you are), like income or sexual orientation. |
| watches a subsidized housing project to identify people, track movements, and record activities of residents. |

Based on a four-item, 5-point Likert-type scale, participants were asked about their opinions on various situations where technology is used in a person’s home for various security purposes such as applying eyeball scan to open locked doors instead of keys or DNA matching to identify strangers who come on the owner’s/renter’s property.

Airline Security. For the context under airline security, participants were given the following prompt: “Airlines are deploying a system that allows passengers to board planes after only a quick security check. This system requires the prior collection of data on passengers.” Based on a four-item, 5-point scale, participants were asked how willing they would be to provide data such as fingerprints, have their eyeballs scanned, and provide their social security number.

Public Safety. To explore perceptions of surveillance technologies with public officials as the agents of control, participants were presented with three situations where public safety officials are considering adopting some technologies (e.g., facial recognition, location tracking, drone-usage, etc.) and asked for their views on the proposed technologies given a 5-point scale.

Privacy Perceptions. Three measures were used to gauge participants’ perceptions about privacy: the extent to which they support surveillance generally, the amount of concern for their personal privacy; and the degree to which people are concerned about the personal information they disclose online being misused.

Misuse of Information. Adapted from Bergström (2015), participants were asked how concerned they were (on a 4-point scale, Not at all concerned to Very concerned) about their information being misused when: searching information on the internet, using e-mail, using social media, using a debit card on the internet, using a virtual assistant voice device like the Amazon Echo or Google Home, and using a mobile phone (α = .88, M = 2.86, SD = 0.73).

Privacy Concern. Using Dinev and Hart’s (2006) privacy concern scale, participants were asked, on a 5-point, Likert-type scale how much they agreed or disagreed with four items: “I am concerned that the information my personal technology gathers about me could be misused,” “I am concerned that a person can find private information about me on the Internet,” “I am concerned about providing personal information through my technology use because of what others might do with it,” and “I am concerned about providing personal information through my technology use because it could be used in a way I did not foresee” (α = .93, M = 4.16, SD = 0.81).

Support for Government Surveillance. Participants’ support for government surveillance was measured by asking participants, on a 5-point scale, the extent to which they favored...
greater government surveillance if it means: reducing national or foreign terrorism; curbing cybersecurity attacks; and if one would receive health care reductions and tax benefits ($\alpha=.91; M=3.53, SD=1.05$).

**Locus of Control.** Rotter’s locus of control scale was adapted to a six-item, 5-point measure that included statements like “In my life, good luck is more important than hard work for success.” and “When I make plans, I am almost certain I can make them work” ($\alpha=0.77$). Items were re-coded such that higher values corresponded with higher external locus of control ($M=2.50, SD=0.67$). We included locus of control as a way to measure generalized self-efficacy in comparison to perceived technology competence, which is a way of measuring specialized efficacy.

**Perceived Technology Competence.** Adapted from Katz and Halpern (2014), perceived technology competence was a seven-item, 5-point scale that asked participants to indicate how much they agreed with statements like “I feel technology in general is easy to operate” and “I keep up with the latest technological developments in my areas of interest” ($\alpha=0.87$). Higher values related to a higher perceived technology competence ($M=3.36, SD=0.84$).

**Results**

The following analysis is broken into a few sections. The first examines different surveillance contexts and explores people’s attitudes toward different types of technology being employed in those situations. The next section reviews attitudes toward two types of biometric technology—DNA identification and facial recognition—and explores the agents of control with and purposes for which people would be more or less comfortable using the technology.

**Comfort With a Range of Privacy-Invasive Technology Across Contexts (RQ1)**

In the following analyses, the situation remained constant while the technology and type of information shared varied. As described in the Method section, the situations were selected based on their alignment with real-life scenarios in which people are often asked to or are required to disclose personal information. They ranged from low-stakes scenarios like a grocery store loyalty program to higher-stakes private and public contexts like one’s home security, airline security, and public safety.

**Grocery Store.** In this scenario, respondents were asked to express their comfort level toward technologies being employed in grocery stores for different situations. As can be seen in Figure 1, 24% of respondents expressed discomfort with wearing a watch while grocery shopping that would monitor their health and provide recommendations on the spot. Twenty percent opposed the idea of in-store cameras that would monitor and log their shopping activity, even if it was for their purposes of understanding their behavior. However, close to 80% of the sample were comfortable with in-store cameras to thwart shoplifters.

**Home Security.** Similar patterns can be observed in respondents’ opinions toward various privacy technologies used in home security. Those systems that are more invasive—DNA matching (28.8%), facial recognition (18.5%), eyeball scanning (17.7%)—were the most resisted (see Figure 2). Alternatively, respondents were more open to the idea of technologies used for security or convenience measures: unique passwords to identify strangers (51.9%), fingerprint scanning to unlock doors (46.9%), and home devices that learn behavior to assist in the household (46.5%).

**Airport Security.** In the airline scenario, respondents were asked what information they would be willing to provide to more efficiently get through security. Respondents were least willing to provide their social security number (30.4%) and most willing to undergo a background check (24.4%). Around half of the sample indicated that they were at least “maybe willing” to provide their fingerprints or have their eyeballs scanned (see Figure 3).

**Public Safety.** In general, around less than half of the sample thought that any of the public safety measures were a good idea. Respondents were most open to public cameras with facial recognition capabilities and less open to drones that could observe activities in public spaces. Respondents were least open to location tracking using mobile phones (see Figure 4).

**Agents of Control and Use-Case (RQ2)**

The percentages of respondents who were more and less comfortable with DNA identification and facial recognition technology are in Tables 1 and 2. Overall, we can see that people are slightly more comfortable with sharing their DNA data than they are with facial recognition technology.

**DNA Identification.** With the DNA identification technology specifically, people are more comfortable sharing their data if they would benefit as a result of sharing: More than half of the sample (55%) were comfortable with a DNA/ancestry company using their DNA sample to determine specific health risks like cancer (55%) and more than a third were comfortable with their DNA sample being used to offer clues about their genealogy (40.5%) and to build a richer health profile about themselves (35%). However, more than 60% of participants were least comfortable in three situations: (1) where their anonymized DNA data would be sold by the DNA/ancestry company to third parties, such as pharmaceutical companies (65.3%), (2) their anonymous DNA profiles
Figure 1. Grocery store scenario: respondents’ comfort level toward technologies being employed in grocery stores for different situations, $N=1,150, 17.19 (4.30)$.

Figure 2. Home-security scenario: respondents’ opinions about various technologies being employed for home security. $N=1,150, 27.77 (8.20)$. 
**Figure 3.** Airport security scenario: respondents' willingness to provide personal information to more efficiently get through security. \( N = 1,150, 11.20 (4.59) \).

**Figure 4.** Respondents' attitudes toward public safety measures employing various technologies for surveillance. \( N = 1,150, 8.62 (3.28) \).
would be sold for paid research projects (63.6%), and (3) if pharmaceutical companies would commercially benefitting from their DNA data (62.3%). Finally, 59% of participants indicated they would be uncomfortable sharing their DNA information with law enforcement, which would allow the agency to look for criminals through DNA matching.

**Facial Recognition.** The types of scenarios in which respondents were more or less comfortable with facial recognition appeared to vary based on the potential utility of and purpose for the data being collected. Respondents were most comfortable if surveillance cameras used facial recognition to distinguish them from other individuals, and for public-utility-oriented outcomes such as if the technology was used by the police to scan crowds in real time for suspicious activities (37.1%), to monitor streets to identify terrorists and to scan for unknown people at the workplace (36.5%). However, respondents were least comfortable with facial recognition when it was employed to build an individual profile about a person for no other use than to have that information collected, such as interpreting one’s facial features to determine income or sexual orientation (21.4% comfortable) and to determine one’s age and gender when shopping (26.7% comfortable). The EFA revealed that the facial recognition items comprised one factor of the 11 items.

**Relationship Between Privacy and Surveillance Technology Perceptions and Comfort With Biometrics (RQ3)**

A regression analysis was conducted to further untangle the dynamics of people’s comfort with these biometric technologies. Three models were constructed (Table 5), controlling for demographics, to determine the extent to which various privacy and surveillance perceptions contributed to level of comfort with: DNA identification for personal benefit; DNA identification for others’ benefit; and overall use of facial recognition technology. The privacy perceptions included were concerns about privacy invasion, concerns about information misuse, and support for public-safety surveillance technology.

The regression models (Table 6) show that individual traits have some, though not very much, influence on comfort with biometric technologies. Men were more comfortable with DNA identification for others’ benefit ($\beta = -0.10, p < .001$).

**Table 5. Contributors to Comfort With Use of Facial Recognition Technology.**

| Variables                        | Model 1 | Model 2 | Model 3 | Model 1 | Model 2 | Model 3 |
|----------------------------------|---------|---------|---------|---------|---------|---------|
|                                  | $\beta$ | $\beta$ | $\beta$ | $\beta$ | $\beta$ | $\beta$ |
| Gender (female)                  | -0.07*  | -0.06*  | -0.05   |         |         |         |
| Age                              | -0.03   | -0.004  | -0.01   |         |         |         |
| Income                           | 0.04    | 0.02    | -0.05   | 0.02    | 0.02    | -0.02   |
| Education                        | -0.01   | -0.03   | -0.001  | -0.01   | -0.01   | -0.01   |
| Black/African American           | -0.04   | -0.04   | -0.02   | -0.05   | -0.05   | -0.04   |
| Hispanic/Latino                  | -0.05   | -0.05   | -0.03   | -0.05   | -0.05   | -0.03   |
| Asian                            | 0.01    | 0.02    | 0.018   | 0.01    | 0.01    | 0.018   |
| Locus of control                 | -0.03   | -0.03   | -0.05   | -0.03   | -0.03   | -0.03   |
| Perceived tech competence        | 0.09**  | 0.05    |         | 0.09**  | 0.05    |         |
| Concern—privacy invasion         | -0.13***| -0.13***|         | -0.13***| -0.13***|         |
| Concern—information misuse       | -0.10***| -0.10***|         | -0.10***| -0.10***|         |
| Surveillance support             | 0.30*** |         |         | 0.30*** |         |         |
| Adjusted $R^2$ (%)               | 0.60    | 1.10    | 13.50   | 2.13*   | 2.61**  | 17.80***|
| $F$                              |         |         |         | 2.96    | 3.20    | 10.77   |

*p < .05; **p < .01; ***p < .001.

**Table 6. Contributors to Comfort With Use of DNA Identification Technology.**

| Variables                        | Individual benefit | Others’ benefit |
|----------------------------------|--------------------|-----------------|
|                                  | Model 1 | Model 2 | Model 3 | Model 1 | Model 2 | Model 3 |
|                                  | $\beta$ | $\beta$ | $\beta$ | $\beta$ | $\beta$ | $\beta$ |
| Gender (female)                  | -0.02   | -0.02   | -0.01   |         |         |         |
| Age                              | -0.12***| -0.13***| -0.11***|         |         |         |
| Income                           | -0.003  | -0.02   | -0.02   | 0.02    | 0.02    | -0.02   |
| Education                        | 0.04    | 0.04    | 0.05    | 0.01    | 0.01    | 0.02    |
| Black/African American           | -0.05*  | -0.05*  | -0.05   | -0.05   | -0.05   | -0.04   |
| Hispanic/Latino                  | -0.03   | -0.02   | -0.02   | -0.05   | -0.05   | -0.03   |
| Asian                            | -0.03   | -0.03   | -0.03   | -0.03   | -0.03   | -0.03   |
| Locus of control                 | -0.08*  | -0.07*  | -0.07*  | 0.07*   | 0.06*   |         |
| Perceived tech competence        | 0.04    | 0.04    | 0.06*   | 0.05    |         |         |
| Concern—privacy invasion         | -0.11***| -0.11***|         | -0.12***|         |         |
| Concern—information misuse       | -0.12***| -0.08** |         |         |         |         |
| Surveillance support             | 0.16*** |         |         |         |         |         |
| Adjusted $R^2$ (%)               | 1.10    | 1.50    | 5.10    | 5.00    | 5.60    | 10.90   |
| $F$                              | 2.96    | 3.20    | 6.81    | 10.77   | 9.52    | 14.08   |

*p < .05; **p < .01; ***p < .001.
Younger people were more comfortable with using DNA identification technology for both individual ($\beta=-0.11, p<.001$) and others’ ($\beta=-0.11, p<.001$) benefit. (Those of Hispanic/Latino race/ethnicity were less likely to be comfortable with DNA identification for others’ benefit ($\beta=-0.013, p<.001$.) Individual efficacy traits were only slightly influential: those with a higher external locus of control were more comfortable with DNA identification technology being used for others’ benefit ($\beta=0.06, p<.05$). Perceived technology competence was not a significant factor in comfort with these technologies. Individual privacy attitudes explained the most variance in comfort with the biometric technologies. The more concerned people are about their privacy being invaded, the less comfortable they are with DNA identification for individual benefit ($\beta=-0.11, p<.001$) and others’ benefit ($\beta=-0.12, p<.001$), and facial recognition technology ($\beta=-0.13, p<.001$). Similarly, the more concerned people are with their information being misused, the less comfortable they are with DNA identification for individual benefit ($\beta=-0.12, p<.001$) and others’ benefit ($\beta=-0.08, p<.01$) and facial recognition technology ($\beta=-0.10, p<.001$). Conversely, the extent to which someone supported surveillance, the more comfortable they were with DNA identification for individual benefit ($\beta=0.07, p<.05$) and others’ benefit ($\beta=0.30, p<.001$), and with facial recognition ($\beta=0.30, p<.001$).

**Discussion**

This study draws from the theoretical perspectives of Nissenbaum’s (2010) contextual integrity and Masur’s (2020) situational privacy by examining how an individuals’ perceived acceptance, willingness, and privacy concerns toward the use of a given biometric technology vary depending on social contexts, specific situations surrounding those contexts, and types of agents in control of the technology. From our first set of results, we found that both the social context and actors wielding the technology mattered for people’s acceptance. Participants’ indication of their willingness to accept even the most invasive types of technology varied depending on the contexts we proposed: airline and home security companies (e.g., private corporations) versus public safety officials (e.g., government).

In the grocery store context, respondents said they were comfortable having biometric technologies in place when the intention of the technology was to detect and thwart shoplifters. They were least comfortable with the idea of providing personalized information for the grocery store to use for personalization and marketing purposes. Similarly for public safety, respondents noted less openness to providing location tracking via mobile phones and more openness to facial recognition technology. This adds to the different aspects of perceptions around personal privacy versus detection of others, in which people may be less willing to disclose their own information particularly if it’s through their mobile phones. However, people showed greater flexibility in using facial recognition technology to detect other people or to protect themselves from others. This outcome can be justified through existing literature’s findings on the interesting interplay between trust-risk trade-offs where people showed greater protectiveness over basic personal information compared with giving away biometrics data when sharing of information was perceived risky (Ioannou, Tussyadiah, & Miller, 2020). Ioannou, Tussyadiah, and Miller (2020) further explain that individuals may perceive behavioral data (i.e., biometrics) as less significant in disclosing sensitive information than identification data (i.e., social security or passport number).

On the flip side, the same respondents noted that using biometric technology to identify strangers and intruders in the context of home security was not a good idea, but that the devices keeping track of personal data for health monitoring or for convenience measures (e.g., automatically opening doors) was a good idea. The two different results here show how social contexts play into perceptions of biometric technology acceptance and openness. The grocery store setting is certainly more public than one’s home. Given this contextual distinction, people may be more open to considering biometrics being used to detect bad behavior of others as these actions of others are something that individuals cannot control in a public setting. People may either prefer to delegate that responsibility to technology or they may feel more confident about their ability to have good intentions, hence the positivity toward technology being used to track down ill-intentioned individuals. However, in a contrasting, private space that is an individual’s home, people may be more protective of privatizing their livelihood and more inclined to control their own agency.

Finally, in the context of airlines, respondents were neutral about providing fingerprints or having their eyeballs scanned to efficiently get through airport security. This sense of indifference and inevitability, which draws from privacy concepts of apathy, resignation, or cynicism (Draper & Turow, 2019; Hargittai & Marwick, 2016; Lutz et al., 2020) may be indicative of the normalized, biometrics security practices that US airports have been enforcing since the 9/11 terrorist attacks. Our results complement existing travel-related privacy research where travelers have greater vulnerability to privacy violations and little awareness of privacy threat given that places such as airports demand both a physical and mental sense of urgency to obtain certain types of personal information in return for people’s ability to travel (Tussyadiah et al., 2019).

Adding to the context variability, a second contribution we make to the literature on situational and contextual privacy is that people are more comfortable with the use of bodily intrusive technology when it explicitly benefits them, such as their health or safety, but not when the situation involves data collection for identification storage. Branching off Masur’s situational perspective on privacy in which his
work revealed that people are more open to self-disclosure in situations when perceived privacy protection is higher, we went deeper and singled out technologies that are often seen as having lower levels of privacy protection (or containing highly sensitive data).

For example, nearly half of our sample respondents said they were comfortable giving away their DNA sample to determine specific health risks; they displayed the most willingness to use DNA identification technology to understand their health and determine genealogy. When it came to facial recognition technology, respondents were least comfortable with facial recognition when it was used to build an individual profile about a person for no other use than to have that information collected. Respondents were most comfortable with surveillance cameras to distinguish themselves from other individuals and for public-utility outcomes—this is in line with our findings in the public safety context.

Previous studies such as Lwin et al.’s (2007) demonstrate that while general privacy concerns can be curbed through clear intent of data usage, these policies are not as effective in the face of highly sensitive information. As such, information congruency (conceptualized as relevant information collected to the business or transaction context) was shown to have an impact on highly sensitive data. Individuals may be more open to sharing highly sensitive information when the collected data are deemed as congruent with the business or product goal (Lwin et al., 2007). Building on these findings, we discovered that among the biometric technologies that are perceived as more intrusive of using bodily data, individual’s level of openness to disclose and share their information was dependent on purpose limitation and proportionality factors: whether a given technology is being used to personally benefit themselves, to detect malicious actors or activities, and if the technology’s use of intent is congruent. Our data show that in both the context-specific and agents of control questionnaires, the framing that a technology will positively impact an individual’s welfare (i.e., for their own wellbeing) yielded greater openness to accepting or using more intrusive technologies.

This follows the proportionality principle (Privacy International, n.d.) in which individuals feel at ease when the technology does not feel threatening and is believed to be used for “good” by any type of agent. This social impact-driven framing can positively impact individual perceptions and transparency on data sharing via certain technologies. However, when data are perceived to be arbitrarily stored without clear intent or is not congruent with the proposed technology use-case, people reacted with negative feedback—regardless of the degree of technology’s technical intrusiveness.

Limitations

This study relied on self-report data, which are subject to a number of validity threats, including response bias. Given the nature of the measures, we can only claim to have captured perceptions of these technologies, rather than actual use or intentions for use. Subsequently, the technologies were described in real-life situations in which they might be employed (e.g., airports, public streets, grocery stores, home security), to increase the study’s ecological validity, but such contextualization limited the consistency across measures and applicability to participants. The questions asked for each scenario were slightly different for the technology and context to make most sense. Therefore, the inconsistency in question wording made it more difficult to make direct comparisons among the four scenarios. It would be interesting to see how results might change if respondents were given uniform knowledge of the risks and claims to efficacy associated with specific biometric technologies. A future survey that experiments with disclosure statements can be informative for activists and researchers who are pushing for greater transparency with regards to the risk these technologies have. Future research can pick apart people’s perception of government surveillance versus private corporation surveillance and if these preferences have clear delineations given other variables such as political ideologies, political systems, cultural differences, and beliefs around race and identity.

Conclusion

Considered together, our results shed light on the complex trade-off between technological innovations and privacy at the individual level as well as society’s systematic infrastructures. To date, biometrics has shifted from the first to second generation of the technology development cycle. Biometrics was initially focused on individual identifiers (i.e., “who you are”), while the second generation moved toward extrapolating individual behaviors (i.e., “how you are”) (Schumacher, 2012). This generational focus shift is not uniquely tied to biometric technology; social media platforms powered by advanced algorithms are also demonstrating similar capacities in which the sheer quantity of individual data allows for intricate observation and prediction of longitudinal behavior. What makes biometrics unique is the technology’s dependence on bodily data as a way to justify its precision in detection and discovery coupled with social media’s ability to hyper-personalize and create networked information patterns. This widened technical capacity is a major technological development, but it comes with great concern and need for caution around the unintended consequences it can inflict on society and individual’s livelihood.

Another inevitably we draw from our work is the effect of normalization (Foucault, 1995). To this day, normalization pervades society through the standardization of governmental programs, medical applications and in the adoption of consumer technology. The advancements and diversity of biometric technologies in the consumer market are normalizing the way people use and perceive the intrusiveness of those technologies. As more consumers accept biometric
technologies into their lives, the highly personal metadata that is hidden behind those technologies become lucrative for multiple agencies involved. This can blur the lines between private corporations and public agencies and introduces the potential for private companies to assist government organizations for reasons beyond what the technology intended for the consumer.

The immediate implications of this normalization effect in biometrics most negatively harm marginalized communities. For years, facial recognition technology used for police surveillance has disproportionately targeted people of color (Samuel, 2022). As such, racial biases and stereotypes are not only embedded, but overtime, enhanced in these technologies through reduction and categorization of physical features (Stark, 2019; Wu & Zhang, 2016). Nonetheless, new biometric technologies will always appear in the market and through governmental efforts to address protection around user and citizen privacy. Worldcoin is an example of a biometric technology initiative that potentially violates the principle of proportionality and purpose limitation in which the company’s stated purpose doesn’t align with their data collection procedure and business actions. Worldcoin was created to revolutionize digital information ownership and decentralize traditional institutions using eyeball scans and cryptocurrency (Blania & Altman, 2021). The founders of Worldcoin frame their technology as a new way to distribute wealth and provide greater citizen prosperity around the world. However, investigations show deceptive business intentions in which the company targeted participants in countries that were most economically vulnerable due to the pandemic and collected individuals’ iris scans and other biometric data in return for social assistance and support (Guo, 2022).

Our study’s focus on context-specific and agents in control differences could be a helpful reference point when evaluating complex issues between the deployment of biometrics and the privacy concern levels of users in certain contexts. From an educational and policy perspective, it would be highly beneficial to inform users and the general public around the implications of technology normalization effects, clearly define the application of biometric technologies, and illustrate how one’s biases around certain social contexts and norms can blur his or her ability to judge the intrusiveness of a technology.

Furthermore, the overarching inevitability we draw from our work is that any type of agent involved in the creation and dispersion of biometric technologies (now and in the future) will have to weigh the cost-benefit of how much transparency they are willing to provide around the technical, data collection scope versus losing or gaining the trust and reliance of users. As technology privacy studies in different contexts have shown, trust-building, risk management, and clear communication strategies are necessary to reduce privacy concerns (Ioannou, Tussyadiah, & Miller, 2020). It is critical for technology developers and agents in control of the technology to conduct a proportionality assessment to mitigate consequences such as chilling effects and misuse of data that contain harmful social biases. This should also be conducted periodically by other third-party agents who can provide objective assessments on how the technology is being used. Accountability or scoring of assessment can be held via media exposure or user feedback mechanisms. Without proactive measures to mitigate the ethical issues of biometric technology before the technology is built or introduced to the public can create long-lasting implications of mistrust, misuse, and unhealthy reliance on the technology’s true capabilities.

Availability of Data and Material
Requests for data can be sent to the corresponding author.

Code Availability
Not applicable.

Consent to Participate
Not applicable.

Consent for Publication
Not applicable.

Declaration of Conflicting Interests
The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Ethics Approval
Study was reviewed and approved for conducting anonymous self-report surveys by the Boston University’s College of Communication research review board (RRB) on January 26, 2021. COM RRB #21034.

Funding
The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iDs
Sejin Paik https://orcid.org/0000-0003-1245-4838
Kate K. Mays https://orcid.org/0000-0002-8477-9634

References
Agre, P. E. (1994). Surveillance and capture: Two models of privacy. *The Information Society, 10*(2), 101–127. https://doi.org/10.1080/01972243.1994.9960162
Alhammad, M. M., & Gulliver, S. R. (2014). Persuasive technology and users acceptance of E-commerce. *Journal of Electronic Commerce in Organizations, 12*(2), 1–13. https://doi.org/10.4018/jeco.2014040101
Apthorpe, N., Shvartzshnaider, Y., Mathur, A., Reisman, D., & Feamster, N. (2018). Discovering smart home internet of things privacy norms using contextual integrity. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 2*(2), 1–23. https://doi.org/10.1145/3214262
Molla, R. (2019, May 13). People say they care about privacy but they continue to buy devices that can spy on them. *Vox*. https://www.vox.com/recode/2019/5/13/18547235/trust-smart-devices-privacy-security

Molla, R. (2020, January 21). Amazon Ring sales nearly tripled in December despite hacks. *Vox*. https://www.vox.com/recode/2020/1/21/21070402/amazon-ring-sales-jumpshot-data

Morosan, C., & DeFranco, A. (2015). Disclosing personal information via hotel apps: A privacy calculus perspective. *International Journal of Hospitality Management*, 47, 120–130. https://doi.org/10.1016/j.ijhm.2015.03.008

Nagourney, A., & Elder, J. (2006, January 27). New poll finds mixed support for wiretaps. *The New York Times*. https://www.nytimes.com/2006/01/27/politics/new-poll-finds-mixed-support-for-wiretaps.html

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

North-Samardzic, A. (2019). Biometric technology and ethics: Beyond security applications. *Journal of Business Ethics*, 167(3), 433–450. https://doi.org/10.1007/s10551-019-04143-6

Norval, A., & Prasopoulou, E. (2017). Public faces? A critical exploration of the diffusion of face recognition technologies in online social networks. *New Media & Society*, 19(4), 637–654. https://doi.org/10.1177/1461444816688986

Phillip Redman, C. (2015, August 7). Biometrics get mobile: Go ahead and touch ID. *Wired*. https://www.wired.com/2014/10/go-ahead-and-touch-id/

Privacy International. (n.d.). *Legality, necessity and proportionality*. https://privacyinternational.org/our-demands/legality-necessity-and-proportionality

Samuel, S. (2022, April 19). Why it’s so damn hard to make AI fair and unbiased. *Vox*. https://www.vox.com/future-perfect/22916602/ai-bias-fairness-tradeoffs-artificial-intelligence

Schumacher, G. (2012). Behavioural biometrics: Emerging trends and ethical risks. In D. Tzovaras & E. Mordini (Eds.), *Second generation biometrics: The ethical, legal and social context* (pp. 215–227). Springer.

Shaffer, G. (2020, December 4). Applying a contextual integrity framework to privacy policies for smart technologies. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3742916

Slobogin, C. (2003, February 24). Public privacy: Camera surveillance of public places and the right to anonymity. *Electronic Journal*. https://doi.org/10.2139/ssrn.364600

Smith, A. (2020, August 27). More than half of U.S. adults trust law enforcement to use facial recognition responsibly. *Pew Research Center*. https://www.pewresearch.org/internet/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly/

Stark, L. (2019). Facial recognition is the plutonium of AI. *XRDS: Crossroads, the ACM Magazine for Students*, 25(3), 50–55.

Taddicken, M. (2013). The “privacy paradox” in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication*, 19(2), 248–273. https://doi.org/10.1111/jcc4.12052

Thompson, S., Davis, A., & Ma, J. (2019, April 11). Where would you draw the line? *The New York Times*. https://www.nytimes.com/interactive/2019/04/10/opinion/privacy-survey.html

Transportation Security Administration. (n.d.). *Biometrics technology*. https://www.tsa.gov/biometrics-technology

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennöhfer, A., & Lind, F. (2015). Do people know about privacy and data protection strategies? Towards the “Online Privacy Literacy Scale” (OPLIS). In S. Gutwirth, R. Leenes, & P. de Hert (Eds.), *Reforming European data protection law* (pp. 333–365). Springer.

Tuss禹iah, L., Li, S., & Miller, G. (2019). Privacy protection in tourism: Where we are and where we should be heading for. In J. Pesonen & J. Neidhardt (Eds.), *Information and communication technologies in tourism* (pp. 278–290). Springer. https://doi.org/10.1007/978-3-030-05940-8_22

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

Westin, A. (1967). *Privacy and freedom*. Ig Publishing.

Wieland, A., Durach, C. F., Kembro, J., & Treiblmaier, H. (2017). Statistical and judgmental criteria for scale purification. *Supply Chain Management: An International Journal*, 22(4), 321–328.

Worthington, R. L., & Whittaker, T. A. (2006). Scale development and ethical risks. In D. Tzovaras & E. Mordini (Eds.), *Second generation biometrics: The ethical, legal and social context* (pp. 479–500). Springer.

**Author Biographies**

Sejin Paik (MA, Stanford University) is a PhD Candidate of Emerging Media Studies at Boston University’s College of Communication. Her research interests include multimodal media effects, human–computer interaction, and the ethics of artificial intelligence in information technologies.

Kate K. Mays (PhD, Boston University) is a postdoctoral researcher at the Autonomous Systems Policy Institute of Syracuse University. Her research interests include human–machine communication, the social impact of emerging technologies, and governance of artificial intelligence.

James E. Katz (PhD, Rutgers University) is the Feld Professor of Emerging Media Studies at Boston University’s College of Communication. His research interests include psychological consequences of social media, public guidance of artificial intelligence, and mobile media studies.