Selected Papers of #AoIR2020:
The 21st Annual Conference of the
Association of Internet Researchers
Virtual Event / 27-31 October 2020

INVASIVE YET INEVITABLE? PRIVACY NORMALIZATION TRENDS IN EMERGING TECHNOLOGY

Sejin Paik
Boston University

Kate K. Mays
Boston University

Rebecca Giovannetti
Boston University

James E. Katz
Boston University

Introduction

In the last few years, smart security and physical identification technologies have grown exponentially; people are increasingly installing smart video devices to monitor their homes and buying DNA kits to collect and analyze their genetics. For example, Amazon Ring (a home security system) nearly tripled sales in a year and about 400,000 Ring security devices were sold just in December 2019 (Molla, 2020). Roughly 25 million individuals have their DNA information incubating in major genetic testing companies such as Ancestry and 23andMe (Bursztynsky, 2019).

As the number of users and profits of these businesses increase, so too does the potential for privacy violations and exploitation. The Electronic Frontier Foundation recently found that Ring partnered with over 500 police departments to provide its data for investigative purposes (EFF, 2019). Similarly, news revealed that Family Tree DNA, another major home DNA kit company, voluntarily works with the FBI to provide their customers' database to assist agents in violent crime cases (Hernandez, 2019). DNA testing companies are expanding their reach beyond public officials by providing users' database access to drug makers, insurance companies and mobile application developers (Hart, 2019a).

Suggested citation (APA): Paik, S., Mays, K. K., Giovannetti, R., Katz, J. E. (2020, October) *Invasive yet Inevitable? Privacy Normalization Trends in Emerging Technology.* Paper presented at AoIR 2020: The 21st Annual Conference of the Association of Internet Researchers. Virtual Event: AoIR Retrieved from http://spir.aoir.org.

As personalized, data-driven devices become more entrenched in people's everyday lives, corporations continue to inject cutting-edge technologies into the consumer market at a fast pace and subsequently, increase the discrepancy between people's concerns about privacy and their actual use of those technologies. From research and consumer reports alike, individuals are overall weary, anxious and alarmed at the potential risks of losing control of their privacy (Molla, 2019). However, there is no clear decline in the sales and uses of these biometric devices; particularly as the factor of convenience and usefulness become a component. One possible explanation for this phenomenon is Foucault's concept of normalization (Foucault, 1995). Normalization today pervades society through the standardization of governmental programs, medical applications, and in the adoption of technology.

Study Purpose

Using normalization as a foundational pillar, 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. Biometric technology itself is not new in 2020; however, it is becoming more popularized and attractive within the consumer market space. Given previous literature and theories on privacy, we move beyond simply looking at people's general intentions and inclinations for technology use tied to privacy concerns. We believe that an individuals' acceptance level towards the use of biometric technologies depends largely on a given situation, physical context and the agent in control of the technology. This paper provides a window into biometrics technology privacy and considers the subtler and nuanced spaces of biometrics technologies' impact on the conceptualization of privacy by individuals and society.

To explore these dynamics of privacy in biometric technology, we conducted a U.S. nationally representative survey (N = 1,587) through the professional survey company Qualtrics in July - August, 2019. We first identified respondents' attitudes toward two types of biometric technology — DNA identification and facial recognition — and examined the agents of control for which people would be more or less comfortable using the technology. Additionally, we provided various surveillance contexts such as grocery stores, home and public safety to understand attitudes towards different types of technology being employed in those situations.

Findings & Discussion

Our analysis shows that the actor wielding the technology matters for people's acceptance. People are more willing to accept even the most invasive types of privacy identification technology if they trust the actor that's employing it. Moreover, respondents were most comfortable with intrusive technology when it explicitly benefited them, such as their health or safety. Nearly half of the sample (44.9%) were comfortable with a DNA ancestry company using their DNA sample to determine specific health risks like cancer. For 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. When keeping the actor constant across privacy technologies, there was an overwhelming preference for less invasive means of privacy data sharing. With that being said, respondents were overall more open to accepting public officials' and airlines' use of more invasive technologies to guarantee people's safety. Most respondents were willing to comply with invasive means such as eyeball and fingerprint scanning and full background checks in order to board a plane, which is a different trend than found among other actors such as grocery stores and home security companies.

From our results, we discuss: 1) the extent to which people have become desensitized and normalized to intrusive technologies; 2) how societal contexts (Nissenbaum, 2010) and agents of control change the way people respond to the use and comfort level toward a given technology; and 3) the privacy versus beneficial trade-offs people are willing to make at the macro and micro-level.

References

No author. (2019, October 22). EFF to Amazon and Shaq: Stop pushing police partnerships with doorbell camera company. Electronic Frontier Foundation (EFF). Retrieved from https://www.eff.org/press/releases/eff-amazon-and-shaq-stop-pushing-police-partnerships-doorbell-camera-company

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. Proceedings of the 5th ACM Conference on Electronic Commerce, 21-29.

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., Turner, E. (2019, November 15). Americans and privacy: Concerned and feeling lack of control over their personal information. Pew Research Center. Retrieved from https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Bursztynsky, J. (2019, February 12). More than 26 million people shared their DNA with ancestry firms, allowing researchers to trace relationships between virtually all Americans: MIT. CNBC. Retrieved from https://www.cnbc.com/2019/02/12/privacy-concerns-rise-as-26-million-share-dna-with-ancestry-firms.html

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use and User Acceptance of Information Technology, MIS Quarterly, 13, 3, 319-340.
Foucault, M. (1995). Discipline and punish : The birth of the prison (2nd Vintage Books ed.). New York: Vintage Books.

Hart, K. (2019a, February 25). Genetic testing firms share your DNA data more than you think. Axios. Retrieved from https://www.axios.com/dna-test-results-privacy-genetic-data-sharing-4687b1a0-f527-425c-ac51-b5288b0c0293.html

Hart, K. (2019b, February 25). Consumers kinda, sorta care about their data. Axios. Retrieved from https://www.axios.com/consumers-kinda-sorta-care-about-their-data-3292eae9-2176-4a12-b8b5-8f2de4311907.html

Hernandez, S. (2019, January 31). One of the biggest at-home DNA testing companies is working with the FBI. Buzzfeed News. Retrieved from https://www.buzzfeednews.com/article/salvadorhernandez/family-tree-dna-fbi-investigative-genealogy-privacy

Li, J., Ma, Q., Chan, A., & Man, S. (2019). Health monitoring through wearable technologies for older adults: Smart wearables acceptance model. Applied Ergonomics, 75, 162-169.

Molla, R. (2019, May 13). People say they care about privacy but they continue to buy devices that can spy on them. Vox recode. Retrieved from 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 recode. Retrieved from https://www.vox.com/recode/2020/1/21/21070402/amazon-ring-sales-jumpshot-data

Nissenbaum, H. (2010). Privacy in context : Technology, policy, and the integrity of social life. Stanford, Calif.: Stanford Law Books.

Norberg, Patricia A., Horne, Daniel R., & Horne, David A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. Journal of Consumer Affairs, 41(1), 100-126.

Pranić, Ljudevit., Roehl, S. Wesley, & West, B. David. (2009). Acceptance and Perceived Effectiveness of Biometrics and Other Airport Security Procedures. 1-23.