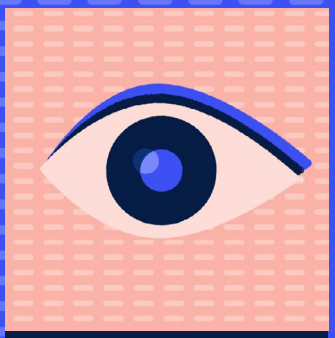


FUTURE DIGITAL THREATS TO DEMOCRACY

This ongoing series from Technology for Global Security and the Center for a New American Security examines the elements and potential implications of digital threats to democracy over the next ten years.

Digital Threats to Democracy: Eye See You

Vera Zakem, Technology for Global Security

WHAT IS PRIVACY, REALLY?

The United Nations Universal Declaration of Human Rights states that privacy is a human right. The violation of this right for any reason puts at risk an individual's sense of security and identity. Privacy can also be viewed as a consumer protection issue. When consumers sign on to new services and products, they want to understand the terms of service for how their data will be protected, used, and shared. Yet, regardless of one's perspective, both individuals and consumers often lack understanding of privacy as a value, even though many are extremely concerned about surveillance, Personal Identifying Information (PII) data leaks, and corporate collection and sharing of their information.

THE THORNY CHALLENGES OF PRIVACY

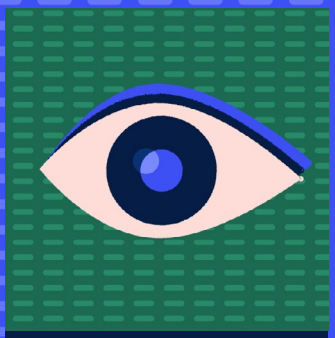
Over the past several decades, technological innovation has created many opportunities for multinational corporations and government institutions to serve customers globally, be it individuals, brands, governments, and civil society. Yet, this innovation has brought with it enormous responsibility and a challenge to protect both individual and consumer privacy. Several unresolved issues pose serious threats to democracy:

- Lack of understanding what really constitutes privacy and data protection
- Difficulty enforcing data regulation
- Malicious actors sharing PII and using technology to infringe on privacy
- Lack of privacy education for all members of society

When it comes to understanding privacy, the Pew Research Center highlights that a quarter of Americans are asked to read a company's privacy statement on a daily basis, but just 9 percent actually take the time before agreeing to the terms of service. Marginalized communities are disproportionately affected; in particular, lower-income populations are less likely to have secure and private personal data. For example, individuals in lower income brackets and without a college education are more likely to say they think their personal information is less secure now than in the past. One potential explanation for this data privacy divide is the motivation to use free apps and services and limited privacy education.

DIFFICULTY ENFORCING DATA PROTECTION LAWS

With mixed understanding of what really constitutes privacy and data regulation, lack of standardization, and international transit of business and data, it is challenging to create and enforce regulation for both government and corporate



FUTURE DIGITAL THREATS TO DEMOCRACY

This ongoing series from Technology for Global Security and the Center for a New American Security examines the elements and potential implications of digital threats to democracy over the next ten years.

entities. Take for instance the European Union (EU) Global Data Protection Regulation (GDPR). This 2018 law sought to limit corporate collection and sharing of user data without explicit user consent. Many in the privacy community viewed GDPR as a model for other countries in enacting and enforcing privacy regulation. However, enforcement of this regulation has been mixed, with varying degrees of interpretation of the law. Enforcing data regulation in the United States has been a mixed bag as well, because U.S. privacy laws are not uniform and are "patched up" together. Further, privacy and data regulations are governed by individual countries and governing international bodies. Regulating corporations and entities that operate in a global market is especially challenging.

NEFARIOUS ACTORS ARE TAKING NOTE

Nefarious actors—individual hackers, corporations, and state actors—have taken note of mixed successes with privacy regulation and lack of overall consumer understanding on privacy. After Russia famously hacked into the Democratic National Committee systems, a new wave of digital asymmetric warfare gained prominence and attention in which adversaries strategically obtain and leak PII. China's subsequent hack of Equifax affected 143 million U.S. citizens. What's more, in our pandemic "new normal," adversaries and allies alike use location tracking and facial recognition technologies to track individual movement. As Katie Josef and Samuel Woolley write, "what unites these efforts is their reliance on data harvested from people's smartphones and other devices—veritable troves of personal information ripe for collection and exploitation."

Further, these actors have been taking advantage of new technologies in facial recognition to further invade privacy for criminal or strategic aims. Technologies such as those developed by Clearview AI could enable easy and widespread surveillance, where a simple app could identify most of the population and use personal data as it pleases. As Kashmir Hill writes, the proliferation of surveillance apps could make "searching someone by face … as easy as Googling a name."

HOPE FOR THE FUTURE?

Whether you view privacy as a basic human or a consumer protection right, one thing is clear: privacy and data governance will likely continue to shape—and potentially undermine—democracies over the next ten years. We will need to focus on solutions that highlight greater understanding, education, and private-public partnerships with emphasis on regulation, information sharing, and iterative lessons learned. Finally, as democracies we are still learning and adapting. Therefore, greater investment in privacy-related research and technology is needed in order to mitigate these concerns and prepare for our likely turbulent future.

Vera Zakem is a Senior Technology and Policy Advisor with Technology for Global Security. She is a recognized leader, driving strategy at the intersection of global threats, policy, emerging technologies and innovation, and organizational strategy and operations.