ENGINEERING A SUSTAINABLE FUTURE

Engineering a Sustainable Future: Privacy and Security in the Age of Smart Technology

by Safayat Moahamad, LL.B, CIPP/C, CIPM, FIP

Published: August 2023

ONTARIO
SOCIETY OF
PROFESSIONAL
ENGINEERS

www.ospe.on.ca

TABLE OF CONTENTS

About the Author 3
Abstract 4
Engineering a Sustainable Future: Privacy and Security in the Age of Smart Technology 5
Introduction 5
The Privacy Component 5
The Cybersecurity Component 6
Sidewalk Labs: A Case Study 6
How Engineers Can Help 7
Bibliography 8

ABOUT THE AUTHOR

Safayat Moahamad, LL.B, CIPP/C, CIPM, FIP

Safayat Moahamad is a Canadian Information Privacy Professional. He was called to the Bar of England & Wales as a member of the Honourable Society of Lincoln's Inn following the completion of the LL.B. program at the University of London. With over 5 years of experience in privacy, legal, and compliance, he has coached teams on information protection across multiple sectors.

Safayat is an avid follower of global privacy and cybersecurity trends, as well as an active advocate of privacy by design and ethical AI. He is experienced in leading globally distributed teams to develop and deliver privacy programs. Inspired by physicists and astronomers, he is passionate about helping organizations that operate at the intersection of innovation, commerce, and governance.

Through various speaking engagements and appearances, Safayat has shared his expertise on privacy and data regulation in Canada, with a particular focus on the evolving landscape shaped by Bill C-27, also known as the Consumer Privacy Protection Act. He has delivered an OSPE ENGtalk on this topic, shedding light on the forthcoming changes. Additionally, Safayat has presented at an IAPP KnowledgeNet talk, discussing the same subject matter, and has spoken about AI, data privacy, and cybersecurity at the ISACA Toronto Annual Summer Conference. He aims to provide organizations with valuable insights and knowledge to effectively prepare for the future in these areas.

ABSTRACT

While smart technologies have the potential to deliver sustainable economic growth and move society forward, they can also threaten to compromise personal autonomy, privacy, and security. This paper will outline the personal and societal risks posed by the rise of smart technologies, and identify how engineers can foster a culture of responsible innovation.

INTRODUCTION

The drive towards a circular economy is expediting the era of smart technologies aimed at optimizing the use of natural resources and lowering carbon emissions. Smart cities, autonomous vehicles (AVs), and the internet of things (IoTs) will play a vital role in promoting conscious consumption, sustainable transportation, and improving efficiency of critical infrastructure.

The Circular Economy[1] may be designed to reduce impacts on the environment, while promoting societal growth and sustainability. It could, nonetheless, result in a lack of personal autonomy as the shift requires change in consumer behaviour. The same smart technologies that promise to move society forward can be leveraged to influence, nudge, and even coerce individuals into conducting themselves in a certain manner, resulting in a reduction of personal autonomy (Ranchordas, 2019).

It is imperative that the transition to a circular economy is inclusive and equitable, and that the benefits derived through ethical use of smart technologies are transparent and accessible to all citizens. The engineering community can help achieve this goal by recognizing the threats of smart technologies and raising awareness about the principles of data protection and Privacy by Design[2].

THE PRIVACY COMPONENT

Smart technologies collect and generate vast amounts of data, including personal information such as real-time location, health data, behaviour patterns, and other sensitive information relating to personal preferences (Yang and Xu, 2018). Mechanisms to capture such data points, and the algorithms used to analyze them, need carefully designed controls and testing.

Without these controls, smart technologies can have detrimental outcomes for individuals and society at large, as privacy is not just an individual right but also a societal value (Nissenbaum, 2010). For example, gaining access to a smart home IoT device could enable a malicious actor to use the device's camera to spy on the owner, or the device's microphones to listen in on conversations, which could result in cyberstalking, cyberbullying, and identity theft. Gartner Inc. has gone as far as to predict that cyber attackers will have weaponized operational technology environments to successfully harm or kill humans by 2025 (Gartner Inc., 2021).

As a result of this rapid convergence of physical and digital ecosystems, engineers need to truly understand how and why data is collected, stored, shared, and used. So that sustainable development goals can be pursued proactively while respecting the right to privacy, by protecting personal information.

[1] *"In a circular economy, nothing is waste. The circular economy retains and recovers as much value as possible from resources by reusing, repairing, refurbishing, remanufacturing, repurposing, or recycling products and materials."*
- *https://www.canada.ca/en/services/environment/conservation/sustainability/circular-economy.html*

[2] *"Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation."*
- *https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf*

THE CYBERSECURITY COMPONENT

In 2013, Miss Teen USA Cassidy Wolf revealed to the FBI that she had been spied on, in her own bedroom, through the webcam of her computer (DailyMail.com, 2014). She had received an email from the perpetrator containing a series of photographs that had been taken over the period of a year. In this case, there was only one computer and one webcam exploited, possibly with just one spyware. But since then, the world of cybercrime has evolved significantly. With massive amounts of data points in transit from smart home IoTs, telemetry from AVs which can now involve brain frequency data, and evolving smart cities laced with sensors and cameras, the threat landscape has only broadened for adults and children alike.

Bear in mind also that threats extend beyond personal information and devices. At a macroeconomic level, cyberattacks can target critical infrastructure systems such as power plants, water treatment facilities, and transportation networks, systems that are essential for the functioning of society. If these systems are compromised, it can result in power outages, contamination of water supplies, and transportation disruptions, all of which can lead to physical harm.

A study conducted at MIT Sloan School of Management found that the healthcare industry is increasingly vulnerable to cyberattacks, which can result in the loss of sensitive information, financial theft, and even compromised medical equipment, leading to the demise of critical patients. Data breaches are estimated to have a collective impact of around $6 billion on the healthcare industry in the United States (Jalali and Kaiser, 2018).

Between October 2019 and June 2020, the Canadian Broadcasting Corporation published two articles noting that healthcare professionals and cybersecurity experts are worried about Canada's health system being constantly targeted by cybercriminals seeking access to sensitive patient information (Burke, 2020). The growing threats overwhelm healthcare facilities, and three Ontario hospitals have already fallen victim to attacks impairing computer systems (Daigle, 2019). This raises concerns about the security of other healthcare facilities as well.

SIDEWALK LABS: A CASE STUDY

The "Sidewalk Toronto" project offers a useful case study for concerns around smart technology and large-scale data collection. Waterfront Toronto and Sidewalk Labs, a subsidiary of Alphabet Inc. (also known as Google), teamed up in 2017 to transform Toronto's 12-acre underdeveloped eastern Quayside into a smart urban area that promised to enhance residents' quality of life. The project's Master Innovation and Development Plan included sustainability ideas such as closely monitoring residential energy consumption and recycling – elaborate systems which could pry into the private activities of individuals.

Bianca Wylie, a prominent Toronto resident and technology / public engagement expert, identified that Sidewalk Labs aimed to create an improvement cycle based on feedback from residents and buy-in from entrepreneurs, rather than relying on city planners and civil engineers (O'Kane, 2022). This approach can be used by tech giants to develop smart products that become essential to people's lives and difficult to regulate.

Further data protection and privacy concerns about Toronto's smart city project were shared by Ontarians Dr. Ann Cavoukian and Jim Balsillie (O'Kane, 2022). Their concerns spanned from the rise of surveillance capitalism (Zuboff, 2019), jeopardizing the Canadian Charter of Rights and Freedoms, to the monetization of intellectual property built on massive data collection from individuals. How the city and its residents would benefit from this project, and what level of control they would have, was largely unclear.

Subsequently, Toronto learned that the plan presented by Sidewalk Labs was only a reduced version of a much larger plan that was leaked. The full plan showed that Sidewalk Labs intended to develop approximately 500 acres in downtown Toronto (O'Kane, 2022). The project was eventually cancelled in 2020.

Having control over such vast amounts of consumer data and personal information – as Sidewalk Labs aimed to do – can enable organizations to nudge human behaviour. "Nudging" is a concept in behavioural economics that refers to the use of subtle cues or environmental design elements to influence an individual's actions. While nudging can be effective in promoting desired behaviours, it is important for organizations to be transparent about the use of personal information and to ensure that nudges are ethical and do not undermine individual autonomy (Ranchordas, 2019).

Additionally, organizations must comply with privacy laws and regulations and take measures to protect the personal information they collect. This includes implementing robust security controls to protect against unauthorized access to personal information, as well as providing individuals with control over their information and the ability to opt-out of nudging or any other privacy-invasive initiatives.

HOW ENGINEERS CAN HELP

Engineers play a crucial role in the design and development of smart cities, AVs, and IoT devices. Thus, it is vital for the engineering community to be aware of the privacy and security risks that may result from these technologies. Engineers can build their understanding through:

- **Training:** Engineers should consider training on privacy and Privacy by Design principles, data protection, and risk management. The International Association of Privacy Professionals (IAPP) offers programs and certifications that are highly recommended.
- **Collaborating:** Engineers can collaborate with privacy professionals (such as privacy lawyers, data protection officers, and consultants) to gain a better understanding of privacy risks and incorporate privacy considerations into the design and development of their technologies at inception.
- **Continuing Education:** Engineers should stay informed about the latest trends in privacy and cybersecurity, such as new laws, regulations, and best practices. This can be done by attending relevant conferences (such as **IAPP**'s Canada Privacy Symposium and **ISACA Toronto**'s Annual Summer Conference) and participating in similar discussion forums. Additionally, obtaining professional credentials as a **Certified Information Privacy Technologist (CIPT)** and **Certified Data Privacy Solutions Engineer (CDPSE)** can be very beneficial.

As privacy and security concerns grow in the pursuit of sustainability, engineers will have the pivotal role in ensuring that smart technologies are designed and implemented with security safeguards and respect the right to privacy.

BIBLIOGRAPHY

[1] Ranchordas, Sofia. “Nudging Citizens through Technology in Smart Cities”, University of Groningen Faculty of Law Research Paper Series No. 1, 2019.

[2] Yang, Fan and Xu, Jian. Privacy Concerns in China’s Smart City Campaign: The Deficit of China’s Cybersecurity Law, Crawford School Research Paper. Asia & The Pacific Policy Studies, Issue 3, Volume 5, 2018.

[3] Nissenbaum, Helen. Privacy in Context: Technology, Policy, and the Integrity of Social Life, Stanford University Press, 2010

[4] Gartner Inc. “Gartner Predicts By 2025 Cyber Attackers Will Have Weaponized Operational Technology Environments to Successfully Harm or Kill Humans”, Press Release, Newsroom, 21 July 2021, https://www.gartner.com/en/newsroom/press-releases/2021-07-21-gartner-predicts-by-2025-cyber-attackers-will-have-we

[5] Daily Mail Reporter. “More than 90 people arrested in ‘creepware’ hacker sting as victim Miss Teen USA describes ‘terror’ at being watched through her webcam for a YEAR”, DailyMail.com, Politics, 25 May 2014, https://www.dailymail.co.uk/news/article-2638874/More-90-people-nabbed-creepware-hacker-sting-victim-Miss-Teen-USA-describes-terror-watched-webcam-YEAR.html

[6] Jalali, Mohammad S. and Kaiser, Jessica. “Cybersecurity in Hospitals: A Systematic, Organizational Perspective”, MIT Sloan Research Paper No. 5264-18, Journal of Medical Internet Research; 2018.

[7] Burke, David. “Hospitals ‘overwhelmed’ by cyberattacks fuelled by booming black market”, CBC News, 2 June 2020, https://www.cbc.ca/news/canada/nova-scotia/hospitals-health-care-cybersecurity-federal-government-funding-1.5493422

[8] Daigle, Thomas. “Here’s what we know about the ransomware that hit 3 Ontario hospitals”, CBC News, 4 October 2019, https://www.cbc.ca/news/science/ransomware-ryuk-ontario-hospitals-1.5308180

[9] O’Kane, Josh. Sideways - The City Google Couldn’t Buy, Random House Canada, 2022.

[10] Zuboff, Soshana. The Age of Surveillance Capitalism, Profile Books, 2019.

[11] Veliz, Carissa. Privacy Is Power, Bantam Press, 2021.

[12] Farahany, Nita A. The Battle for Your Brain: Defending the Right to Think Freely in the Age of Neurotechnology, St. Martin’s Press, 2023.

[13] Ziosi, Marta, and Hewitt, Benjamin, and Juneja, Prathm, and Taddeo, Mariarosaria, and Floridi, Luciano. “Smart Cities: Reviewing the Debate about their Ethical Implications”, SSRN, Smart Cities, 5 January 2022, Available at SSRN: https://ssrn.com/abstract=4001761 or http://dx.doi.org/10.2139/ssrn.4001761

[14] Finch, Kelsey and Tene, Omer. “Smart Cities: Privacy, Transparency, and Community”, Cambridge Handbook of Consumer Privacy, Eds. Evan Selinger, Jules Polonetsky and Omer Tene, 2018, Available at SSRN: https://ssrn.com/abstract=3156014

[15] Moody, Ryan. “Defending Against Cyberattacks on Operational Technology”, Forbes, Innovation, 28 October 2021, https://www.forbes.com/sites/forbestechcouncil/2021/10/28/defending-against-cyberattacks-on-operational-technology/?sh=1d958e1e5e76

[16] Laville, Sandra. “Greta Thunberg effect’ driving growth in carbon offsetting”, The Guardian, Climate Crisis, 8 November 2019, https://www.theguardian.com/environment/2019/nov/08/greta-thunberg-effect-driving-growth-in-carbon-offsetting

ENGINEERING A SUSTAINABLE FUTURE

CONTACT US

Ontario Society of Professional Engineers
4950 Yonge Street, Suite 502
Toronto, Ontario M2N 6K1
1-866-763-1654

www.ospe.on.ca

ONTARIO
SOCIETY OF
PROFESSIONAL
ENGINEERS