INSIGHT 8

AI FURTHER ERODES PRIVACY

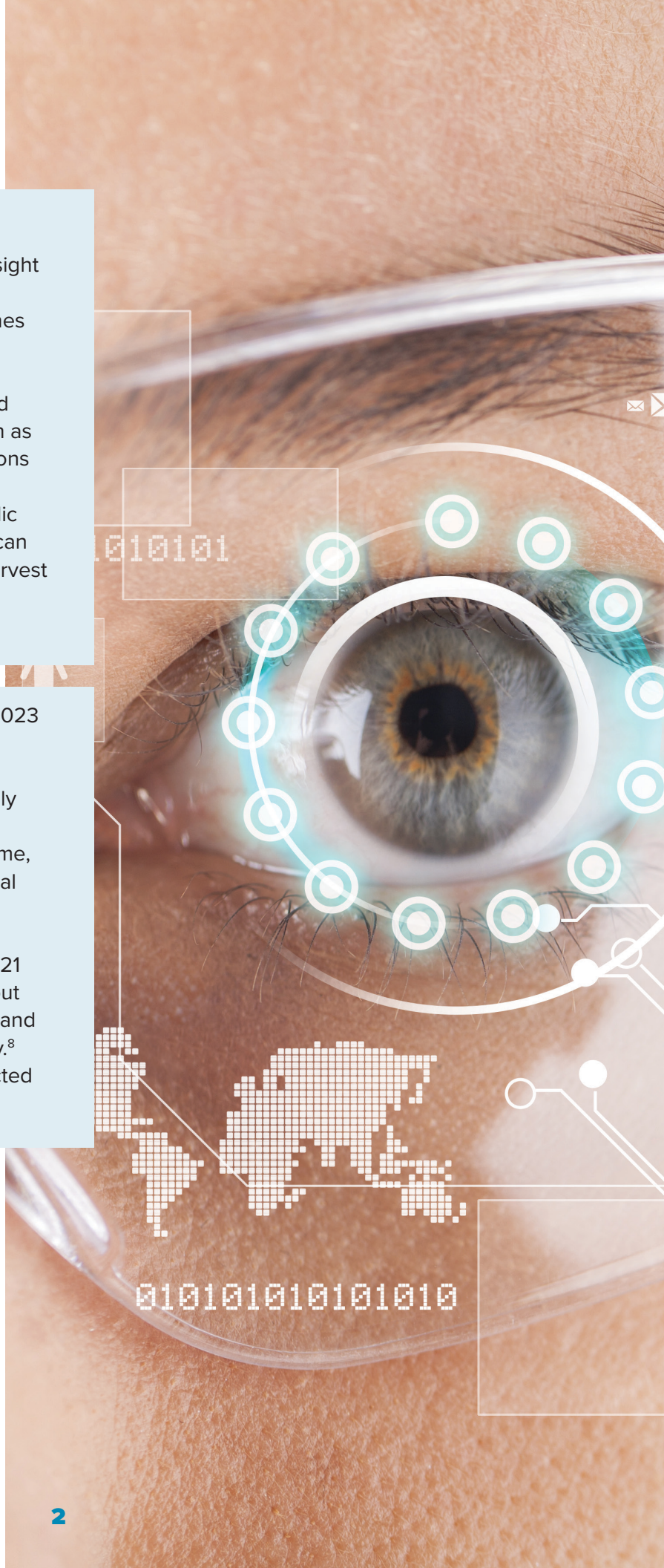
As AI-enabled devices collect more data online and in real life, efforts to turn data into new revenue streams could butt up against more privacy-conscious attitudes and devices. A new status quo may emerge that looks very different from the opaque way that users today exchange their data for free services.

TODAY

Advances in AI are exacerbating privacy issues with technology. Most Canadians have become accustomed to accessing free online services – such as social media sites, generative AI platforms, or mobile apps. In many cases, they unknowingly give consent to companies to collect their data, sell it to third parties, and use AI to make sense of it and draw inferences about them. For example, Facebook uses AI to make inferences about users' suicide risk based on their social media posts.[1] Improvements in AI are allowing firms to analyze a greater variety and amount of data and transform it into revenue streams in new ways.

Not only online environments but also physical spaces are becoming less private. As noted in Insight 7, everyday household objects are outfitted with sensors to collect data – from toilets to toothbrushes to toys. Virtual Reality (VR) and video games can collect data about users' behaviour in the home and use AI to make inferences about emotions and personality traits.[2] Outside the home, devices such as smart glasses[3] and AI pins[4] are raising new questions about privacy in public. Fragments of human DNA, known as environmental DNA, collected from public spaces for purposes such as disease monitoring, can potentially be used to track individuals, illegally harvest genomes, and engage in hidden forms of genetic surveillance and analysis.[5, 6]

Smart cars raise particular privacy concerns. In 2023 the Mozilla Foundation investigated 25 car brands and found that every one collected personal data that is not necessary to operate the vehicle[7], usually taken from mobile devices connected to cars via apps, this data can include a person's annual income, immigration status, race, genetic information, sexual activity, photos, calendar, and to-do list. Of the 25 brands, 22 use this data to make inferences – for example, from location and phone contacts – and 21 share or sell data. Thirteen collect information about the weather, road surface conditions, traffic signs, and "other surroundings", which can include passersby.[8] Ninety-five percent of new vehicles will be connected vehicles by 2030.[9]



FUTURES

As the Internet of Things becomes the "AI of Things", data may become even more valuable, further incentivizing ever more data extraction. It may become possible to draw more sophisticated inferences to predict human behaviour, movement, or identify individuals, as discussed in Insight 5.

However, international regulatory pushback could reshape the privacy landscape. More jurisdictions are passing and enforcing new data privacy laws[10], such as the American Privacy Rights Act[11] in the US. This could change some, if not many, aspects of "surveillance capitalism"[12] by giving users more control over their data. Future legal reforms could reframe inferences as personal information[13], making it more difficult to sell them to third parties.

Emerging technology could also shift the privacy balance. Edge computing, which refers to networks or devices that are physically near to the user, could enhance data privacy and security.[14] When user data is stored and processed on a user-owned device, it may be more difficult for companies to collect and sell it.[15] However, edge computing can also introduce new risks, such as enabling face recognition on local devices and potentially easier access for malicious actors.[16]

IMPLICATIONS

- **Distinctions** such as public versus private and online versus offline could become **increasingly blurred**. Homes and other spaces could be experienced as more or less private depending on the use of devices. Visitors to homes and passengers in cars may demand **new consent protocols to protect their privacy**
- Data shared with third parties could lead to **sensitive information being shared** with insurance companies[17]
- Schools and childcare providers could **use privacy protections as a competitive advantage** to attract families
- Surveillance could change the **practices of police and criminals**
  - Some forms of crime could move further underground and become more organized to evade detection
  - New technological capabilities could create new opportunities for hacking, fraud, and stalking
  - Traffic police may be less needed as monitoring of drivers by governments and insurance companies enables tickets to be issued automatically
- Activists[18] and journalists[19] could increasingly use ubiquitous computing to "return the gaze" by **collecting information about powerful organizations or individuals**. This practice is known as "sousveillance" or "equivalence." This could include hacking sensitive information about the personal lives of political representatives or other public figures[20]
- Data protection regimes could become **more complex** and less aligned globally
- Jurisdictions could struggle to balance privacy with researchers' need for representative datasets in areas such as medicine[21]
- Jurisdictions with weaker privacy laws could become increasingly "risky" destinations for work or travel
- **Privacy-protecting devices** could tilt the balance of power toward users

Endnotes

1 Singer, Natasha. In Screening for Suicide Risk, Facebook Takes On Tricky Public Health Role. The New York Times, December 31, 2018, sec. Technology.

2 Kröger, Jacob Leon, Philip Raschke, Jessica Percy Campbell, and Stefan Ullrich. Surveilling the Gamers: Privacy Impacts of the Video Game Industry. Entertainment Computing 44 (January 1, 2023): 100537.

3 Chen, Brian X. How Meta's New Face Camera Heralds a New Age of Surveillance. The New York Times, December 13, 2023, sec. Technology.

4 Brianna R. Humane AI: Privacy Implications of This New AI-Powered Lapel. Medium (blog), December 22, 2023.

5 Jenny While, Jessica Alice Farrell, and The Conversation. The DNA You Shed Could Identify You. Scientific American, May 15, 2023.

6 Whitmore, Liam, Mark McCauley, Jessica A. Farrell, Maximilian R. Stammnitz, Samantha A. Koda, Narges Mashkour, Victoria Summers, Todd Osborne, Jenny Whilde, and David J. Duffy. Inadvertent Human Genomic Bycatch and Intentional Capture Raise Beneficial Applications and Ethical Concerns with Environmental DNA. Nature Ecology & Evolution 7, no. 6 (June 2023): 873–88.

7 Caltrider, Jen, Misha Rykov, and Zoe MacDonald. It's Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy. Privacy Not Included by Mozilla (blog), September 6, 2023.

8 Caltrider, Jen, Misha Rykov, and Zoe MacDonald. It's Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy. Privacy Not Included by Mozilla (blog), September 6, 2023.

9 McKinsey. Unlocking Connected Cars with Corporate Business Building. August 31, 2023.

10 Rimol, Meghan. Gartner Identifies Top Five Trends in Privacy Through 2024. Gartner Press Release (blog), May 22, 2022.

11 Hunton Andrews Kurth. New Bipartisan Federal Privacy Proposal Unveiled: American Privacy Rights Act, April 23, 2024.

12 Zuboff, Shoshana. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. Public Affairs, 2019.

13 Office of the Privacy Commissioner of Canada. Principles for Responsible, Trustworthy and Privacy-Protective Generative AI Technologies, December 7, 2023.

14 Schulze, Kris. Cloud Computing vs. Edge Computing | Blog. Scale Computing, May 2, 2024.

15 Earney, Shandra. Is the Edge or Cloud Better for Security and Privacy? Xalient, October 17, 2022.

16 Swabey, Pete. Why Edge Computing Is a Double-Edged Sword for Privacy. Tech Monitor (blog), March 31, 2023.

17 Beasy, John, Chris Hagerman, Amanda Joy, Nicole Rigillo, Simon Robertson, Tieja Thomas, Kristel Van der Elst, and Meaghan Wester. Future Lives: Uncertainty. Ottawa: Policy Horizons Canada, 2024.

18 Miller, Lloyd. RECON VILLAGE - Applied OSINT For Politics: Turning Open Data Into News - TIB AV-Portal. Presented at the DEF CON, Las Vegas, 2018.

19 Vincent, Subramaniam. How Open Source Intelligence Can Help Journalists Cover Conflicts. Markkula Center for Applied Ethics (blog), October 3, 2023.

20 Pierson, Chris. Celebrities Are a Big Target for Hackers - Cyber Threats. BlackCloak | Protect Your Digital LifeTM (blog), October 15, 2020.

21 Lobel, Orly. The Problem With Too Much Data Privacy. Time Magazine, October 7, 2022.

PDF: PH4-218/2025E-PDF
ISBN: 978-0-660-76895-3

Aussi disponible en français sous le titre : L'IA compromet encore plus la vie privée.