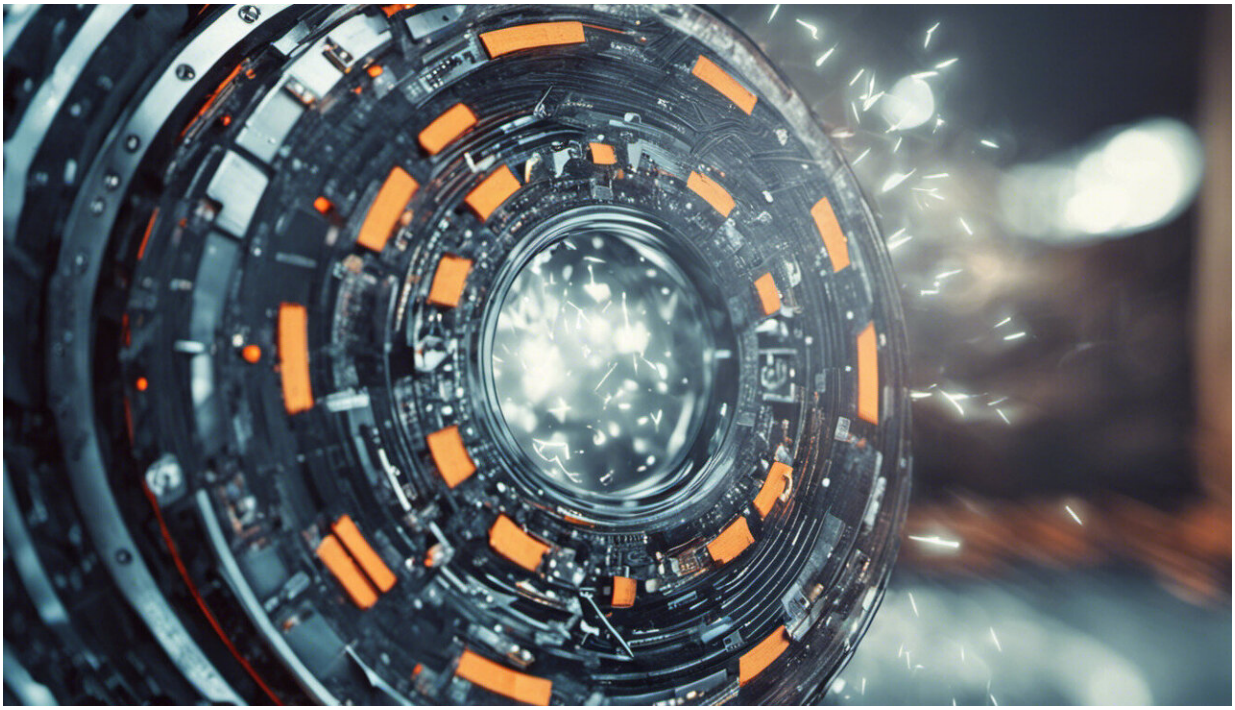
Protecting privacy online begins with tackling 'digital resignation,' say researchers

March 3 2023, by Meiling Fong and Zeynep Arsel



Credit: AI-generated image (disclaimer)

From smart watches and meditation apps to digital assistants and social media platforms, we interact with technology daily. And some of these technologies have become an essential part of our social and professional lives.

In exchange for access to their digital products and services, many tech companies collect and use our personal information. They use that information to predict and influence our future behavior. This kind of surveillance capitalism can take the form of recommendation algorithms, targeted advertising and customized experiences.

Tech companies claim these personalized experiences and benefits enhance the user's experience, however the vast majority of consumers are unhappy with these practices, especially after learning how their data is collected.

'Digital resignation'

Public knowledge is lacking when it comes to how data is collected. Research shows that corporations both cultivate feelings of resignation and exploit this lack of literacy to normalize the practice of maximizing the amount of data collected.

Events like the Cambridge Analytica scandal and revelations of mass government surveillance by Edward Snowden shine a light on data collection practices, but they leave people powerless and resigned that their data will be collected and used without their explicit consent. This is called "digital resignation".

But while there is much discussion surrounding the collection and use of personal data, there is far less discussion about the modus operandi of tech companies.

Our research shows that tech companies use a variety of strategies to deflect responsibility for privacy issues, neutralize critics and prevent legislation. These strategies are designed to limit citizens' abilities to make informed choices.

Policymakers and corporations themselves must acknowledge and correct these strategies. Corporate accountability for privacy issues cannot be achieved by addressing data collection and use alone.

The pervasiveness of privacy violations

In their study of harmful industries such as the tobacco and mining sectors, Peter Benson and Stuart Kirsch identified strategies of denial, deflection and symbolic action used by corporations to deflect criticism and prevent legislation.

Our research shows that these strategies hold true in the tech industry. Facebook has a long history of denying and deflecting responsibility for privacy issues despite its numerous scandals and criticisms.

Amazon has also been harshly criticized for providing Ring security camera footage to law enforcement officials without a warrant or customer consent, sparking civil rights concerns. The company has also created a reality show using Ring security camera footage.

Canadian and U.S. federal government employees have recently been banned from downloading TikTok onto their devices due to an "unacceptable" risk to privacy. TikTok has launched an elaborate spectacle of symbolic action with the opening of its Transparency and Accountability Center. This cycle of denial, deflection and symbolic action normalizes privacy violations and fosters cynicism, resignation and disengagement.

How to stop digital resignation

Technology permeates every aspect of our daily lives. But informed consent is impossible when the average person is neither motivated nor

knowledgeable enough to read terms and conditions policies designed to confuse.

The European Union has recently enacted laws that recognize these harmful market dynamics and have started holding platforms and tech companies accountable.

Québec has recently revised its privacy laws with Law 25. The law is designed to provide citizens with increased protection and control over their personal information. It gives people the ability to request their personal information and move it to another system, to rectify or delete it (the right to be forgotten) as well as the right to be informed when being subjected to automated decision making.

It also requires organizations to appoint a privacy officer and committee, and conduct privacy impact assessments for every project where personal information is involved. Terms and policies must also be communicated clearly and transparently and consent must be explicitly obtained.

At the federal level, the government has tabled Bill C-27, the *Digital Charter Implementation Act* and is currently under review by the House of Commons. It bears many resemblances to Québec's Law 25 and also includes additional measures to regulate technologies such as artificial intelligence systems.

Our findings highlight the urgent need for more privacy literacy and stronger regulations that not just regulate what is permitted, but also monitor and make accountable the firms who breach consumer privacy. This would ensure informed consent to data collection and disincentivize violations. We recommend that:

1. Tech companies must explicitly specify what personal data will

be collected and used. Only essential data should be collected and customers should be able to opt out of non-essential data collection. This is similar to the EU's General Data Protection Regulation to obtain user consent before using non-essential cookies or Apple's App Tracking Transparency feature which allows users to block apps from tracking them.

2. Privacy regulations must also recognize and address the rampant use of dark patterns to influence people's behavior, such as coercing them into providing consent. This can include the use of design elements, language or features such as making it difficult to decline non-essential cookies or making the button to provide more personal data more prominent than the opt-out button.
3. Privacy oversight bodies such as the Office of the Privacy Commissioner of Canada must be fully independent and authorized to investigate and enforce privacy regulations.
4. While privacy laws like Québec's require organizations to appoint a privacy officer, the role must also be fully independent and given the power to enforce compliance with privacy laws if it is to be effective in improving accountability.
5. Policymakers must be more proactive in updating legislation to account for the rapid advances of digital technology.
6. Finally, penalties for non-compliance often pale in comparison to the profits gained and social harms from misuse of data. For example, the U.S. Federal Trade Commission (FTC) imposed a $5 billion penalty on Facebook (5.8 percent of its 2020 annual revenue) for its role in the Cambridge Analytica scandal.

While this fine is the highest ever given by the FTC, it is not representative of the social and political impacts of the scandal and its influence in key political events. In some cases, it may be more profitable for a company to strategically pay a fine for non-compliance.

To make tech giants more responsible with their users' data, the cost of

breaching data privacy must outweigh the potential profits of exploiting consumer data.

Provided by The Conversation