Rethinking privacy in the age of psychological targeting

“Psychological targeting” is the practice of predicting people’s psychological profiles from their digital footprints (e.g. their Facebook profiles, transaction records or Google searches) in order to influence their attitudes, emotions or behaviours with the help of psychologically informed interventions. For example, knowing that a person is extroverted makes it possible to personalise recommendations in a way that aligns with their personal needs and preferences for social activities.

The technology of psychological targeting gained global infamy in the context of the Cambridge Analytica scandal in 2016. According to news reports, the company had extracted the psychological profiles of millions of Facebook users – most of them without consent – to discourage them from voting for Hillary Clinton using psychologically tailored messaging.

Although the Cambridge Analytica scandal was the first time that psychological targeting captured public attention, it was not the first time that psychological targeting was introduced. Facebook itself had patented a similar technology in 2012, and researchers (like us) had been studying the feasibility and effectiveness of psychological targeting for a couple of years.

In fact, together with other colleagues we had run and published a number of studies showing that psychological traits such as personality can be accurately predicted from people’s digital footprints such as their Facebook Likes and status updates, their spending records, their browsing histories and many more. We had also shown that such predictions could be used to increase the effectiveness of targeted advertising, with people being more likely to click on ads and to purchase products when targeted with psychologically-tailored messages. And we had publicly talked about both the opportunities as well as the risks of such technological advances. However, it took a scandal like that of Cambridge Analytica for people to finally listen. Our most recent publication discusses the implications of psychological targeting for privacy and data protection. It was born out of the desire to help policy makers, businesses and societies at large tackle the challenges associated with psychological targeting.

Psychological targeting challenges traditional notions of privacy

Date originally posted: 2019-11-21

Permalink: https://blogs.lse.ac.uk/businessreview/2019/11/21/rethinking-privacy-in-the-age-of-psychological-targeting/

Blog homepage: https://blogs.lse.ac.uk/businessreview/

The ability to predict people's intimate psychological traits from seemingly innocuous, passively collected digital footprints, and to subsequently influence their behaviour, poses numerous privacy challenges. One of these challenges results from the fact that the lines between what is public and private become increasingly blurred. For example, a Facebook user might be willing to publicly endorse their favourite brands or news sites using Facebook Likes. However, the same user might consider inferences of personality or political orientation that can be made on the basis of Facebook Likes private. Consequently, the same Likes might be considered to reveal public or private information depending on the context. This problem is further aggravated by the fact that once a piece of information (e.g. a picture or a post) has been publicly shared, it becomes almost impossible to make it private again or remove its digital trace entirely.

A second challenge concerns the fact that psychological targeting has rendered the practice of notice and consent – a cornerstone of most current data protection approaches – outdated and insufficient. It is no longer enough to ask users to agree to lengthy "terms and conditions". Today's privacy landscape is more complex and difficult to understand than ever before. As a result, most people are ill-equipped to make informed privacy decisions that are in their best interest. They simply lack the necessary knowledge to detect which data could potentially be (ab)used to reveal intimate information about them. For example, without a deeper understanding of the inferences one can draw from GPS data (e.g. depression or socio-economic status), a user might unwittingly give away their data without truly understanding the implications of that decision.

Rethinking privacy in the age of psychological targeting: context matters

Given the challenges posed by psychological targeting, we argue that privacy debates need to change fundamentally. They need to move beyond the questions of *who* collects *what* kind of data, to *how* the data are being used. What matters most is context: How are personal data being used, and what are they being used for?

Privacy is violated when data are used in a context or for a purpose that is different from what the user had originally consented to (this concept of privacy is known as contextual integrity and was developed by philosopher Helen Nissenbaum). For example, a user might feel comfortable to publicly share their interests on Facebook. However, they might not agree for these data to be used in predictive models that turn their Facebook *likes* into highly intimate psychological traits. Similarly, a user might be willing to share their data in order to receive personalised advertising for their favourite sporting events. However, the same user might be opposed to sharing their data for personalised advertising in the context of political campaigns. In fact, only 37 per cent of social media users consider targeting in the context of political messaging acceptable, while 75 per cent approve of it in the context of event recommendations. (Pew Research Center, 2018)

The way forward

Scandals such as the case of Cambridge Analytica have put pressure on governments to enforce stronger regulation and oversight. The European Union's General Data Protection Regulation (GDPR) is the first regulation that mentions the concept of "profiling" – and is one of the strictest data protection regulations around the world. At its centre lies the principle of transparency – mandating that companies must disclose in clear and simple terms what type of data is being collected and, most importantly, for what purpose.

Although regulations like the GDPR can support the protection of privacy, they are unlikely to be enough. There is currently a huge discrepancy between individuals' attitudes towards privacy and their observed behaviour (known as the privacy paradox). For example, although 93 per cent of US Americans consider being in control of who can access information about them as important (Pew Research Center, 2015), only a small fraction ever reads privacy policies, and most are more than willing to consent to companies using their data without much thought.

One potential solution to the privacy paradox is direct regulation of psychological targeting, for example prohibiting its use for political campaigning. Another potential solution is privacy by design, which advocates for the proactive integration of privacy and data protection into the design, development and application of new technologies. For example, instead of opting out of specific terms if they do not want their data to be used for a specific purpose, users might be required to opt in if they want their data to be used. By changing the default privacy setting to a level that assures a reasonable degree of protection, the burden of actively protecting their privacy would be lifted from users.

Date originally posted: 2019-11-21

Permalink: https://blogs.lse.ac.uk/businessreview/2019/11/21/rethinking-privacy-in-the-age-of-psychological-targeting/

Blog homepage: https://blogs.lse.ac.uk/businessreview/

Adequate application of psychological targeting can promote trust, allow us to focus on the opportunities of psychological targeting rather than the challenges and lead to disclosure by choice in exchange for better services. We believe that, when implemented in an ethical way, psychological targeting has a vast potential to improve people's lives in all kinds of domains, for example by helping people who suffer from depression to get the personalised support they need.

♣♣♣

- *This blog post is based on the authors' paper* Privacy in the age of psychological targeting. Current Opinion in Psychology, Volume 31. February 2020.
- *The post gives the views of its authors, not the position of LSE Business Review or the London School of Economics.*
- *Featured image by geralt, under a Pixabay licence*
- *When you leave a comment, you're agreeing to our Comment Policy*

Sandra Matz is an assistant professor of management at Columbia Business School in New York. As a computational social scientist, she studies human behaviour and preferences using a combination of big data analytics and traditional experimental methods. Her research aims at understanding how psychological characteristics influence real-life outcomes in a number of business-related domains (e.g. financial well-being, consumer satisfaction or team performance), with the goal of helping businesses and individuals to make better decisions.

Ruth Elisabeth Appel is a PhD student at Stanford University's department of communication, focusing on media psychology. She received a master's in public policy from Sciences Po Paris and a B.Sc. in economics from the University of Mannheim. She is interested in the intersection of behavioural science and computer science, with the aim of leveraging psychological targeting ethically and for the common good. She is particularly passionate about encouraging prosocial behaviour and political participation and promoting wellbeing and mental health.

Michal Kosinski is an associate professor at Stanford University's Graduate School of Business studying the psychological differences between people. He holds a doctorate in psychology from the University of Cambridge and master's degrees in psychometrics and in social psychology. He employs big data and computational models to address pressing issues, including privacy risks, psychometrics, online mass persuasion, and psychological profiling.

Date originally posted: 2019-11-21

Permalink: https://blogs.lse.ac.uk/businessreview/2019/11/21/rethinking-privacy-in-the-age-of-psychological-targeting/

Blog homepage: https://blogs.lse.ac.uk/businessreview/