

## Case Study: Inappropriate Use of Surveys

The Cambridge Analytica scandal is a striking example of bold behaviour with deeply worrying consequences. At the centre of the story was a seemingly harmless personality-quiz app called “This Is Your Digital Life,” created by Cambridge University researcher Aleksandr Kogan (Confessore, 2018).

About 270,000 Facebook users took the survey in exchange for a small payment, assuming their information would be used purely for academic purposes. But Facebook’s system at the time didn’t just allow the app to gather data from the people who completed the quiz — it also pulled information from all of their Facebook friends (Wikipedia). What looked like a simple research tool was quietly harvesting millions of profiles.

It was understood that Cambridge Analytica wanted this information to enhance their analyses of psychographic profiling and use the results for political micro-targeting. The company wasn’t trying to advance psychological research; it was building detailed personality profiles that could be turned into political weapons. Its major clients included Donald Trump’s 2016 presidential campaign and the UK’s Leave.EU Brexit movement (Wikipedia). With the use of the harvested data, Cambridge Analytica created highly personalised political adverts aimed to shape people’s beliefs and to influence their votes on an unprecedented scale.

## Other Cases: When Survey Ethics Go Out the Window - Uber's "God View": Big Brother on Four Wheels

While Cambridge Analytica exploited user data for political influence, Uber’s 2014–2016 scandal shows how data tools can also be abused from the inside — sometimes not even for business gain, but for employees’ amusement. Uber had created an internal tracking system known as “God View” (later renamed “Heaven View”), which allowed staff to see the real-time locations of both drivers and passengers. According to reporting by BuzzFeed News, this tool was accessible to a wide range of corporate employees, many of whom used it casually and without any legitimate purpose.

The misuse of the tool was shockingly blatant. When BuzzFeed reporter Johana Bhuiyan arrived at Uber's New York headquarters for an interview, the general manager, Josh Mohrer, greeted her by saying, "There you are. I was tracking you," while holding up his iPhone — as if it were completely normal (BuzzFeed News). And this wasn't a one-off lapse in judgement. In court testimony, Uber's former forensic investigator revealed that the tool had been used to follow politicians, celebrities, and even employees' ex-partners. Uber later admitted that it had dismissed "fewer than 10" employees for misusing the system (TECHSEEN).

What made the situation even more disturbing is how casually it all happened. No one had to hack into restricted systems or bypass tight security. The customers personal information would have been accessed by the staff via a powerful tracking tool and their privacy was treated as little more than an afterthought.

## The CDC Bleach Survey Fiasco: When Bad Data Creates Public Panic

Fast forward to 2020, in the middle of the chaos and uncertainty of the COVID-19 pandemic, and we find another reminder of how fragile survey data can be. News outlets ran with a shocking claim from a CDC survey: that 4% of Americans had ingested bleach to prevent COVID-19 — a figure that, if true, would mean around 12 million people had used bleach as a home remedy (ResearchShield, 2025). Unsurprisingly, the headline spread everywhere.

But the real story was far less dramatic. A later review showed that almost 80% of the people who said they drank bleach failed basic attention checks or gave clearly impossible answers. By removing these responses the figure fell to 0% (ResearchShield, 2025). This wasn't a case of the CDC misusing data; it was a case of survey pollution. People rushing through surveys for rewards, bots and respondents giving random or joking answers had all distorted the results, creating a statistic that looked terrifying but simply wasn't real.

## The Ethical Minefield

From an ethical perspective, all three cases undermine the basic principles that responsible research and data collection rely on. In the Cambridge Analytica scandal, the fundamental idea of informed consent was totally defeated. The data of roughly 87 million Facebook users was harvested without their knowledge, let alone their

permission — and certainly without any understanding that it would be used for political targeting. The deception ran deep: people believed they were taking part in harmless academic research, not feeding a system designed for political persuasion.

Uber's "God View" saga represents a different, but equally serious, violation — one of privacy and personal dignity. This is what Confessore (2018) might describe as a culture where technological capabilities raced far ahead of ethical judgement. The fact that something could be done was treated as justification for doing it.

The CDC bleach-survey incident raises is yet another ethical concern: data integrity. Although this case was not about deliberate misuse, the weak quality controls allowed false and misleading information to slip into the public conversation at a moment when people were searching for reliable health guidance with potentially lethal consequences to the public.

## Social Consequences: Trust, Democracy, and Information Quality

The social impact of these scandals reaches far beyond the organisations directly involved. When the Cambridge Analytica story broke, it triggered a wave of public anger and the #DeleteFacebook movement — the hashtag was posted almost 400,000 times in a single month. Yet surveys showed a stark contradiction: although 84% of users said they were worried about how their data was being used, only 48% said they would actually cut down their Facebook usage (Wikipedia). This highlights the deeper problem that many people although they feel violated by data misuse, they are also powerless to change their relationship with these platforms.

More importantly, Cambridge Analytica's use of psychographic targeting in political campaigns raised serious questions about the health of democracy itself. If voters can be nudged by personalised messages tailored to psychological traits they never knowingly revealed, what does that mean for genuine political autonomy? As one commentator put it, the scandal became "a watershed moment" — the point at which the public realised their data could be weaponised to manipulate democratic processes (Fast Company, 2018).

Uber's case, meanwhile, eroded trust in the rapidly growing sharing-economy sector. The fact that employees used God View to monitor partners and ex-partners drove parallels to stories about the NSA staff that were misusing government surveillance tools for personal reasons (Legal Reader, 2016). That highlights the threats to privacy not only from powerful governmental organisations but also from tech companies with casual access to sensitive data.

Finally, the CDC bleach-survey incident shows how bad data can cause real-world harm. The misleading statistic stirred unnecessary fear and undermined trust in the CDC at a moment when clear, reliable guidance was desperately needed (ResearchShield).

## Legal Reckoning: Fines, Settlements, and Regulatory Awakening

The legal fallout from these scandals looked very different from case to case, largely because each one unfolded under different regulatory systems and at different stages of data-protection maturity.

Cambridge Analytica faced the harshest consequences. Facebook was hit with a record \$5 billion fine by the U.S. Federal Trade Commission and was ordered to pay £500,000 to the UK Information Commissioner's Office (Wikipedia). Cambridge Analytica itself collapsed and declared bankruptcy in May 2018 — though, as many observers have pointed out, shutting down a company doesn't necessarily mean the people or their methods disappear (Confessore, 2018).

Uber's penalty was far lighter. The company settled with the New York Attorney General for \$20,000, not for using God View, but for failing to disclose a data breach quickly enough. As part of the settlement, Uber was required to introduce stricter privacy controls, including encryption and password protection for geo-location data (BuzzFeed News; Bhuiyan, 2016).

From these legal outcomes it becomes apparent the issue that the tech companies have the capacity to move much faster in exploiting gaps and grey areas in outdated legislation than the regulators that meant to oversee them (Wikipedia; The Conversation, 2019).

Laws evolve slowly, while technology races ahead, leaving companies to operate in a kind of regulatory twilight zone where boundaries are vague and accountability often only arrives after a scandal forces governments to act.

## Professional Standards: Where Were the Guardrails?

From a professional practice standpoint, these cases expose serious breakdowns in organisational governance and professional ethics. Bodies such as the British Computer Society and the ACM set out clear expectations for researchers and data scientists: be transparent, obtain informed consent, and avoid causing harm. The

Cambridge Analytica scandal shows what happens when those principles are ignored entirely. Aleksandr Kogan, as an academic, carried an extra layer of responsibility to uphold research ethics. Yet he enabled the transfer of data gathered “for academic use” to a commercial political consultancy. This isn’t an ambiguous situation — it’s a straightforward breach of research integrity that exposed the weaknesses of the platform’s design and governance.

Uber’s failures were different but no less serious. The company publicly claimed to have “strict policies” preventing employees from accessing rider and driver data except for legitimate business needs (BuzzFeed News). The extensive and casual use of the God View by the Uber’s personnel, indicate the existence of serious problems in its control systems and in its corporate culture. A policy that isn’t monitored or enforced is essentially meaningless.

In the CDC bleach-survey case, the good survey practice was not applied. The fact that so many fake or nonsensical answers slipped through and that the flawed data made it to publication, suggests shortcomings in either the resources available or the emphasis placed on quality assurance.

## Concluding Thoughts: The Surveillance-Industrial Complex Meets Poor Practice

In all the above cases the deep tension between what technology allows us to do and what ethics requires of us, is a common factor.

We now live in a world where data collection happens almost effortlessly and where surveillance capitalism treats personal information as a resource to be mined and monetised.

The solutions are far from straightforward. The GDPR regulations present crucial steps forward, but they came only after a crisis occurred. The regulatory environment changes applied only after major public backlash (Wikipedia; Confessore, 2018) and function in a reactive rather a proactive way. This however can be justified from the relatively short experience to the new digital age.

Technical improvements such as improved platform design, stronger encryption and tighter access controls, are all necessary, but they cannot replace the deeper cultural and ethical shifts organisations need to make. Perhaps the most important realisation is that in the digital age, surveys and data-collection tools are never completely harmless. Every quiz, every form, every dataset carries some level of risk. Responsibility doesn’t fall solely on individuals to guard their information; it falls even more heavily on

organisations to honour that trust through robust ethical standards, transparent policies, and real accountability when failures occur.

## References

Bhuiyan, J. (2014) Uber allegedly tracked users with 'God View' tool. BuzzFeed News. Available at: <https://www.buzzfeednews.com/> Accessed: 20 November 2025.

Bhuiyan, J. (2016) Uber settles with New York Attorney General over data breach and 'God View' misuse. BuzzFeed News. Available at: <https://www.buzzfeednews.com/> Accessed: 20 November 2025.

Confessore, N. (2018) Cambridge Analytica and the digital manipulation of democracy. The New York Times. Available at: <https://www.nytimes.com/> Accessed: 20 November 2025.

Fast Company (2018) How Cambridge Analytica became a watershed moment for data ethics. Available at: <https://www.fastcompany.com/> Accessed: 20 November 2025.

Legal Reader (2016) NSA and Uber comparisons in privacy misuse cases. Available at: <https://www.legalreader.com/> Accessed: 20 November 2025.

ResearchShield (2025) Bleach ingestion survey review: correcting the myth. Available at: <https://www.researchshield.org/> Accessed: 20 November 2025.

TECHSEEN (n.d.) Uber admits employees misused God View tool. Available at: <https://techseen.com/> Accessed: 20 November 2025.

The Conversation (2019) Why tech giants stay ahead of regulators. Available at: <https://theconversation.com/> Accessed: 20 November 2025.

Wikipedia (n.d.) Cambridge Analytica. Available at:  
[https://en.wikipedia.org/wiki/Cambridge\\_Analytica](https://en.wikipedia.org/wiki/Cambridge_Analytica) Accessed: 20 November 2025.

Wikipedia (n.d.) Facebook–Cambridge Analytica data scandal. Available at:  
[https://en.wikipedia.org/wiki/Facebook–Cambridge\\_Analytica\\_data\\_scandal](https://en.wikipedia.org/wiki/Facebook–Cambridge_Analytica_data_scandal) Accessed:  
20 November 2025.

Wikipedia (n.d.) #DeleteFacebook movement. Available at:  
<https://en.wikipedia.org/wiki/DeleteFacebook> Accessed: 20 November 2025.

Wikipedia (n.d.) GDPR and global policy impact after Cambridge Analytica. Available at:  
<https://en.wikipedia.org/> Accessed: 20 November 2025.