Preserve personal freedom in networked societies

Broad anti-discrimination laws and practices could compensate for failing data protection and technology-linked loss of privacy, says **Christoph Bock**.

Surveillance is no longer the prerogative of government agencies. It is privatized, decentralized — and often self-inflicted. Mobile phones trace where we go and with whom we communicate. Smartwatches measure heart rates and will soon start logging happiness and anger. The resulting data are streamed over vulnerable networks to commercial servers; they may be used by advertising companies or shared on social networks.

Current data-protection laws are not prepared for this new reality. Conceptualized in the 1970s and 80s, they were designed for a society that perceived official government databases as the main privacy risk. Their focus on centralization, parsimony and secrecy clashes with today's reality of ubiquitous personal data, deliberate sharing in social networks and all-too-frequent data leaks.

We are quick to blame naive users and careless software developers when personal data are compromised, but the truth is that prudent individual behaviour provides little protection from networked surveillance. Even if I stop using my mobile phone to navigate the digital and physical world, I will still appear in the records of the people around me.

Emerging technologies aggravate the situation. Camera drones watch us from above. Augmented-reality games such as *Pokémon Go* allow developers (or their sponsors) to control where we go in the real world. And handheld DNA sequencers will not only enable real-time monitoring of airborne pathogens (and exciting citizen-science projects), but also reveal our genetic data to anybody who can obtain our DNA.

PRUDENT INDIVIDUAL BEHAVIOUR PROVIDES LITTLE PROTECTION FROM NETWORKED SURVEILLANCE.

Large data sets as substrates for computer algorithms and machine-learning technology assist our daily lives — suggesting where to eat, which book to read and how to stay healthy. But they can be used against us, for example by predicting credit risk or the likelihood of committing a crime. Such predictions can be remarkably accurate, but they struggle with unusual behaviour and often discriminate against minorities. This emergent discrimination is difficult to avoid because it is rarely hard-coded into the algorithms but arises from biased training data. People might start to 'act mainstream' just to be on the safe side — certainly not desirable for a pluralistic society.

So how can we mitigate the inherent risks that 'big data' pose for personal freedom, as billions of connected devices churn out personal data, and data protection by secrecy has become an illusion?

We must remember that data protection is a means to an end, rather than a goal in itself. We do not protect data because the data would take harm; rather, we seek to protect the rights and well-being of individuals who might be harmed by certain uses of their data. This observation could hold the key to protecting personal freedom in a world of evaporating privacy. Finding ways to tame harmful uses of personal data would make future data leaks and unguarded data sharing less of a threat. We can distinguish between essentially financial risks, defined by damages that could be fully compensated through (potentially large) financial payments, and social risks, which affect interpersonal relationships in a way that cannot be reduced to monetary transactions.

Financial risks include higher health-insurance premiums due to genetic risk factors, or waiting longer in a service hotline because the address or a prediction algorithm indicates a low-value customer. Strong anti-discrimination and consumer-protection laws can mitigate these risks, especially when combined with protection for whistle-blowers who uncover violations, and hardship funds that provide compensation when a perpetrator cannot pay.

Social risks include shaming by friends and family over compromising video footage, or attacks over a personal opinion that has become public. Social risks are hard to tackle by legislation, as individuals are unlikely to sue family members for fair and equal treatment. Nevertheless, anti-discrimination laws help mitigate social risks by sending an authoritative message that certain types of discrimination are inappropriate, creating a spillover effect into aspects of our everyday lives not normally controlled by laws and litigation.

Strong anti-discrimination laws thus emerge as a cornerstone of personal freedom when data protection fails and secrecy is compromised by ubiquitous data sharing. The European Union's Charter of Fundamental Rights shows that such protection is legally and politically achievable, prohibiting discrimination by "sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation". The Canadian Human Rights Act also provides relatively broad protection. But the situation is much more fragmented in the United States, and insufficient in China, Japan and large parts of the developing world.

Scientists can contribute to ensuring that the loss of privacy through technology does not result in loss of personal freedom. First, they can credibly assess current and future privacy risks of new technologies and stress the need to move beyond the unsustainable concept of data protection by secrecy. Second, they should advocate for robust legal protection against discrimination around the world. Third, they should educate, advise and monitor, to make sure that facts — not fears — dominate the political debate. ■

Christoph Bock *is a principal investigator at the CeMM Research Center for Molecular Medicine of the Austrian Academy of Sciences in Vienna.*
e-mail: cbock@cemm.oeaw.ac.at