

How governments use Big Data to violate human rights

January 14 2019, by Andrew Thompson



Women in totalitarian states are among those particularly at risk by government's use of Big Data to spy on its citizens. Credit: Matthew Henry/Unsplash

The right to privacy has become a pressing human rights issue. And rightly so. Big data —combined with artificial intelligence and facial

recognition software —has the capacity to intrude on people's lives in unprecedented ways, in some cases on a massive scale.

While much of the discussion has focused on how [social media](#) and [tech companies](#) use the data they collect about their users, more attention needs to be paid to the wider relationship between violations of [privacy](#) and other types of human rights abuses.

The reason is simple. Mass invasions of privacy can undermine the rights of millions, if not billions, of people around the world as governments gain a greater capacity to discriminate —or worse —across gender and sexuality lines, and stifle dissent, including through violence. More about this in a moment.

So what can be done to limit the human rights fallout? What we need is a multi-pronged approach that involves [civil society](#), the private sector, foundations and states.

Establishing human rights funds

First, foundations that support human rights should establish human rights and technology funds. Activists are already harnessing new technologies to monitor and document abuses. Amnesty International is working with a data analysis company to quantify levels of [misogyny on Twitter](#). This type of innovation should be encouraged *and* resourced.

Second, states should negotiate new norms and laws for the digital age. The [Montreal Declaration on the Responsible Use of Artificial Intelligence](#) offers a powerful statement on the need for the ethical development of [new technologies](#). Similarly, the UN Rapporteur on the Right to Privacy is leading efforts to develop what's been called a "[Draft Legal Instrument on Government-led Surveillance and Privacy](#)." These initiatives, and others like them, should be supported.

Third, states must reaffirm the principle of the right to asylum. States that use technology to violate human rights will displace people. Those with a well-founded fear of persecution will need protection.

Finally, states that believe in a rules-based international order must redouble efforts to tackle impunity. Human rights abuses occur because those who commit the violations are rarely held to account. This needs to change.

'Grave consequences'

Failure to check invasions of privacy enabled by technology will have grave consequences. Here are four examples that illustrate this point.

Women's Rights: Surveillance technologies are often used to police morality, especially in places where there is no clear distinction between "sin" and law.

Take Saudi Arabia. In 2017, [Human Rights Watch](#) reported that Saudi courts are using the "vague provisions" in the anti-cybercrime law to "sanction people suspected of committing sexual relations outside marriage, including adultery, extramarital and homosexual sex."

Women are paying a disproportionately high price for these intrusions.

LGBTQ Rights: According to the [International Lesbian, Gay, Bisexual, Trans and Intersex Association \(ILGA\)](#), 72 countries prohibit same-sex relations. Surveillance technologies give governments the ability to "out" individuals. They know where people sleep at night, and with whom. The potential for lives to be destroyed is very great, indeed.

Torture: The governments that violate privacy to suppress minorities are often the same governments that will not think twice about using

torture to maintain control of their citizens. [Syria is a case in point.](#)

Extrajudicial Executions: If governments can track their citizens' movements, it is not difficult to have them assassinated. The Jamal Khashoggi killing is a tragic example of this. The [New York Times](#) has reported that the Saudis used the Pegasus spying software to eavesdrop on Khashoggi, thus enabling his murder.

Other governments could interpret a lack of any meaningful response as permission to target journalists. This is not a hypothetical concern. [According to IFEX](#), an organization dedicated to protecting free expression, 78 journalists were murdered in 2018, and another 159 were imprisoned.

This is not hyperbole. States of all stripes are collecting data on their citizens, and have been for quite some time. This is not going to end any time soon. Quite the opposite.

If left unchecked, invasions of privacy enabled by [technology](#) could put every other human right at risk, and on a scale that would be truly terrifying.

This article is republished from [The Conversation](#) under a Creative Commons license. Read the [original article](#).

Provided by The Conversation

Citation: How governments use Big Data to violate human rights (2019, January 14) retrieved 24 April 2024 from <https://phys.org/news/2019-01-big-violate-human-rights.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is

provided for information purposes only.