



Nov 06, 2018

Categories:

[Blogs](#)

[Podcast](#)

[Publications](#)

[Technology Blog](#)

Authors:

[Joseph J. Dehner](#)

Data Privacy Detective Podcast – Episode 27 – Digital Authoritarianism

“The internet is growing less free around the world, and democracy itself is withering under its influence.” So begins an October 2018 report from Freedom House, a U.S.-based think tank that tracks government control of the internet in the United States and abroad.

The internet was once viewed as an instrument of freedom. It freed communications across borders, aided people’s ability to rally against repressive governments, and dramatically lowered entry barriers for sellers of goods and services across borders. But like many good things, the internet has been increasingly harnessed to repress – or, more neutrally, to assist government authorities in maintaining their power, while keeping a watchful eye and long arm over those who threaten their view of public order.

The Freedom House report is a disturbing compilation of the rise of digital authoritarianism. The study examined 65 countries that hold 87% of the world’s internet users and found a decline in freedom from June 2017 to May 2018 in 26 nations, compared with 19 countries said to have gained freedoms during that same period. Much of the decline relates to efforts by those in power to sway elections that could jeopardize their control. Examples include:

- Venezuela – pre-election laws to arrest people for inciting “hatred” online and implementation of a “Fatherland Card” keeping social data about residents.
- Cambodia – a surge of arrests and incarcerations for online speech.
- Kenya – disinformation targeting voters and up to 10-year prison sentences for people whose posts could result in “panic” or “discredit the reputation of a person”

Notably, in countries as large as China, India, Russia and the United States, internet freedoms declined. China’s 2018 Cybersecurity Law, the numerous “standards” that followed, and its requirement of data localization were accompanied by crackdowns on views at variance with those held by leadership (including websites that

listed Taiwan as a country or quotes from the Dalai Lama). In addition, China's "Great Firewall," as well as its drive to control online platforms within the country and its development of population-wide surveillance and a "social credit index" form, demonstrate the internet's power when used by a government to restrict rather than expand freedom. For this reason, Freedom House's charges that China is "remak[ing] the world in its techno-dystopian image."

Like China, India now insists on data localization, requiring the personal data of its citizens to be kept and stored within India rather than exported. Data localization, often justified as a means of ensuring its residents' data privacy, creates trade barriers and inhibits international communication. Furthermore, cyberattacks on India's domestic stores of personal data offer no proof that keeping data within India actually protects the privacy of its people.

Russia's data localization law similarly aims to keep personal data about Russian citizens within its borders. The country's antiterrorist legislation, effective July 2018, requires telecom and other firms to provide the Federal Security Service (FSB) full access to the content of users' online communications for six months and to register users under their real names for purposes of allowing identification by law enforcement agencies.

These examples are cause for alarm, and yet there are winds of freedom as well. The passage of the GDPR, for instance, and the adoption of broad data protection laws in over 35 countries give residents more control over their personal data than ever, or at least more legal protections and remedies than previously provided, despite the increasing threat of private hackers. The two highest rated countries on the freedom scale, Estonia and Iceland, use innovative technology (including blockchain) to authenticate and encrypt data files, in addition to notifying citizens when their data files are being accessed by government agencies for purposes other than limited investigations requiring advance non-notification.

The Freedom House report concludes with recommendations for policymakers, the private sector, and civil society generally. It's well worth a read.

For more information, please contact [Joe Dehner](#) or any attorney in Frost Brown Todd's [Privacy and Information Security Law Practice Group](#).

To share your thoughts or questions about this or other Data Privacy Detective podcasts, send a message to info@thedataprivacydetective.com. And remember – protecting your personal information begins with you.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.