Bruce Schneier
BT

IT for Oppression

Whether it's Syria using Facebook to help identify and arrest dissidents or China using its "Great Firewall" to limit access to international news throughout the country, repressive regimes all over the world are using the Internet to more efficiently implement surveillance, censorship, propaganda, and control. They're getting really good at it, and the IT industry is helping.

We're helping by creating business applications—categories of applications, really—that are being repurposed by oppressive governments for their own use:

- What is called censorship when practiced by a government is content filtering when practiced by an organization. Many companies want to keep their employees from viewing porn or updating their Facebook pages while at work. In the other direction, data loss prevention software keeps employees from sending proprietary corporate information outside the network and also serves as a censorship tool. Governments can use these products for their own ends.
- Propaganda is really just another name for marketing. All sorts of companies offer social media–based marketing services designed to fool consumers into believing there is "buzz" around a product or brand. The only thing different in a government propaganda campaign is the content of the messages.
- Surveillance is necessary for personalized marketing, the primary profit stream of the Internet. Companies have built massive Internet surveillance systems designed to track users' behavior all over the Internet and closely monitor their habits. These systems track not only individuals but also relationships between individuals, to deduce their interests so as to advertise to them more effectively. It's a totalitarian's dream.
- Control is how companies protect their business models by limiting what people can do with their computers. These same technologies can easily be co-opted by governments that want to ensure that only certain computer programs are run inside their countries or that their citizens never see particular news programs.

Technology magnifies power, and there's no technical difference between a government and a corporation wielding it. This is how commercial security equipment from companies like BlueCoat and Sophos end up being used by the Syrian and other oppressive governments to surveil—in order to arrest—and censor their citizens. This is how the same face-recognition technology that Disney uses in its theme parks ends up identifying protesters in China and Occupy Wall Street protesters in New York.

There are no easy technical solutions, especially because these four applications—censorship, propaganda, surveillance, and control—are intertwined; it can be hard to affect one without also affecting the others. Anonymity helps prevent surveillance, but it also makes propaganda easier. Systems that block propaganda can facilitate censorship. And giving users the ability to run untrusted software on their computers makes it easier for governments—and criminals—to install spyware.

We need more research into how to circumvent these technologies, but it's a hard sell to both the corporations and governments that rely on them. For example, law enforcement in the US wants drones that can identify and track people, even as we decry China's use of the same technology. Indeed, the battleground is often economic and political rather than technical; sometimes circumvention research is itself illegal.

The social issues are large. Power is using the Internet to increase its power, and we haven't yet figured out how to correct the imbalances among government, corporate, and individual interests in our digital world. Cyberspace is still waiting for its Gandhi, its Martin Luther King, and a convincing path from the present to a better future. ■

Bruce Schneier is the chief security technology officer of BT. His latest book is *Liars & Outliers*. He can be found online at www.schneier.com.

Copublished by the IEEE Computer and Reliability Societies