Surveillance, Privacy, and You.

Solomon Greenberg 2017/01/01

If you have nothing to hide, you have nothing to fear. Or, at least, that's what you've been told. The reality is much less straightforward, and more concerning. With the advent of our fully interconnected planet, we're seeing more and more governments and corporations around the world attacking and stripping away their citizens' individual privacies. Of course, this is always in the name of some bogeyman — counter-terrorism being en vogue . Unfortunately, the almost nonexistent pros to digital surveillance and the demolishment of privacy don't outweigh the cons. The argument for safety through surveillance is an all too common one in our modern time, one that threatens to strip away our personal liberties.

Easily the most grossly over-hyped threat to the security of Americans these days is that of terrorism. A late 2015 Gallup poll puts the percentage of Americans either "Very worried" or "Somewhat worried" of a terrorist attack on their family at 51%. The probability that any given American is destined to die at the hands of a terrorist one in 3.6 million, as calculated by the Cato institute. This discrepancy is extensively exploited to push agendas, especially the pervasive one that more digital surveillance and the removal of privacy can help fight terrorism. However, this argument, the core of pro-surveillance side of the debate on privacy, is, and has been shown to be deeply and fundamentally false.

In 2001, after the 9/11 attacks, the US Congress passed the USA PATRIOT Act, which dramatically increased govt. agencies' warrant-less power. This bill was marketed as the de facto standard for counter-terrorism. In theory, it would allow government agencies to crack down on terrorism faster and more efficiently. In practice, it allowed government agencies to expand surveillance programs and nearly cast aside the fourth amendment. To this day, the prevention of not even a single attack has been credited to the USA PATRIOT Act. This is the perfect example of the slippery slope in the privacy debate. Novelist Kenneth Eade stated "The Patriot Act has practically obliterated the Fourth Amendment to the Constitution. It was supposed to be temporary, but there are so many things that the Government likes about the power that it gives, they keep renewing it."

But, as we've all been told, violation of privacy is no reason to be worried unless you have something to hide; hence the mantra of "nothing to hide, nothing to fear." Now, in a perfect world, this would be a valid argument. Unfortunately, ours is anything but, and anything but remaining vigilant and fighting against any infringements of our rights will set us further on the slippery slope of surveillance. Edward Snowden stated "Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say," saying one should not cast aside their rights just because they're not currently using them, like we're seeing so much of in the modern day.

And more than just a fundamental right, the right to privacy can be thought of as the right to self. When once has control over their privacy, they have control and sole knowledge and control over the more personal matters of their life. As well, surveillance can be disastrous if the data falls into the wrong hands. In 2015, 21.5 million people's data was stolen after a government breach, including SSNs. Even without a 1984-esque surveillance network, data breaches can have disastrous consequences., not to mention the potential for blackmail, coercion, and slander possible when a malcontent has access to the wrong databases.

So what can one do to prevent their privacy from being breached in today's world? Vote. The number one thing one can do is to be informed and to vote for people who will uphold the Constitution and citizens' privacy. As well, people would do well to consider using a Virtual Private Network — a service that easily anonymizes the user on the internet. Finally, one should is move away from

commercial computer operating systems such as Microsoft Windows and Mac OSX, both of which have been shown to be vulnerable to government attacks. Windows 10 even has been recorded as constantly broadcasting privacy-infringing data to Microsoft. One alternative is the GNU/Linux operating system, a free and open source OS that currently powers most servers and phones in the wold, and is a fitting desktop replacement for Windows and OSX, carrying a myriad of benefits over both.

Unfortunately, we are living in an age where privacy is becoming devalued, and surveillance is creeping into our everyday lives under the guise of safety. Only through logical thinking and vigilance can we maintain our rights and liberties in the modern world, and protect them for future generations.