Richard Stallman: The Vanishing State of Privacy

* * * * *
We are now subject to a greater level of surveillance than any point in history, and most of it is thanks to the digital revolution of the last few decades. Lucy Ingham hears from the legend Richard Stallman about how the digital transformation has dramatically eroded our privacy, and what it means for our lives
* * * * *

The digital revolution has enriched our lives in so many ways, giving us access to information and capabilities our ancestors only dream of. But that has come at a price: surveillance. Companies that provide us with the services we use know an incredible amount about us, from what we're reading and where we go, to who we vote for and what our hobbies are.

Most of us aren't keen on this, but we accept it as an unavoidable part of the modern world, if we even think about it at all. The data collected on us is part of the digital ecosystem in which we live, and most of us accept that it's an unavoidable part of modern reality.

Richard Stallman, president of the Free Software Foundation, programming legend and recipient of at least 15 honorary doctorates and professorships, however, doesn't think so. He has dedicated his professional life to railing against software surveillance, and despite surveillance continuing to increase in prevalence every year, he remains as strong a voice on the subject as ever.

At the end of 2016, Stallman gave a talk at Web Summit where he outlined the case against software surveillance in the modern world. Addressing a crowd heaving with programmers and yet exceptionally short on journalists – I was the only one – he was his eccentric self, standing with only socks on his feet, dramatically overrunning his timeslot and concluding with the auction of a soft toy wildebeest – known also as a gnu – before vanishing into the night with an army of software disciples following in his wake.

Many too easily dismiss Stallman as an irrelevant oddity, but to do so would be to ignore the very serious and compelling points he raises. For while the rest of us accept the growing lack of privacy afforded to us, Stallman sheds light on how utterly strange and wrong we would have found it even a short while ago.

"Privacy is extremely important. When a great hero, Edward Snowden, informed us of how much the government was snooping on our web browsing, the rate of access to certain Wikipedia pages fell by 20%. Pages like Al Qaeda, bombs," he says. "These people, they were not terrorists but they were afraid that the government would treat them as terrorists if they were seen looking up certain topics in the encyclopaedia. So people are intimidated by the knowledge that they're being watched all the time."

So often we think of a loss of privacy as unimportant, but Stallman argues it is quite the opposite, striking at the very roots of the democratic world in which we exist.

"It threatens democracy more directly. Democracy means that people control what the state does, but first we have to know what the state does; the state tends to hide its actions, and the only way we find out is through whistleblowers," he explains.

“But the government doesn't want people to find out about its nasty, perhaps criminal behaviours, so the government declares the whistleblower to be a spy and a traitor, and tries to put the hero in prison.

“If the government can identify the whistleblower, it’s too dangerous for the whistleblower. If we want to find out what the state is doing so that we the people can have control over it, we need to make whistleblowers safe. But if the government can tell who goes where and who talks to who, there's no way for the journalist's source, the whistleblower, to talk with the journalist and have the government not know.

“So we must reduce the level of data collection of our people down to point where the state can't tell who's talking with journalists. Any system of data collection that enables the state to find out who talked with that journalist is a deadline threat to democracy. And no matter what supposed secondary service this data collection serves, we can't, we don't dare, permit it to continue.”

Proprietary software: the driver of unprecedented surveillance

For Stallman, the reason for this data collection is that the market has been dominated by proprietary software, which prevents users from seeing, or making changes to, the code under the hood.

“The reason that we are subject now to more surveillance than there was in the Soviet Union is that digital technology made it possible,” he says. “And the first disaster of digital technology was proprietary software that people would install and run on their own computers, and they wouldn't know what it was doing.

“They can't tell what it's doing. And that is the first injustice that I began fighting in 1983: proprietary software, software that is not free, that the users don't control.”

Here, Stallman is keen to stress, he doesn’t mean free in the sense of not costing money – plenty of free software is paid for – but free in the sense of freedom to control. Software, after all, instructs your computer to perform actions, and when another company has written and locked down that software, you can’t know exactly what it is doing.

“You might think your computer is obeying you, when really its obeying the real master first, and it only obeys you when the real master says its ok. With every program there are two possibilities: either the user controls the program or the program controls the users,” he says.

“It's free software if users control it. And that's why it respects their freedom. Otherwise it's a non-free, proprietary, user subjugating program.”

The reason that we are subject now to more surveillance than there was in the Soviet Union is that digital technology made it possible

According to Stallman, for software to qualify as free it must provide what he describes as “four essential freedoms”.

“Freedom zero is to run the program however you wish, for whatever purpose you have. Freedom one is the freedom to study and change the source code,” he explains.

Source code is particularly important, because when proprietary software is downloaded by a user, it comes as executable code, such as an exe file on Windows.

“Source code, that's like a mixture of English and math; if you've learned that programming language you can read it and understand it, and then you can change it,” he explains. “But to run it we convert it into executable code, which is very hard for anybody to understand. That's called reverse-engineering. So practically speaking, in order for users to study and change the program, they've got to have the source code.”

These two freedoms allows users to individually control their own copies of software, and tailor it to their needs, however they aren’t much use for those of us who can’t program. Which is where freedoms two and three come in, as they are designed to provide collective control, or “the freedom to work in a group to exercise control over what the program does”.

“Collective control is the way that non-programmers can participate deciding what the program can do,” he explains. “It requires two more freedoms: freedom two is to make exact unmodified copies and give or sell them to others when you wish. And freedom three is to make copies of your modified versions and give or sell them to others when you wish.

“So when the program carries these four freedoms, the users control it, it respects their freedom, that's free software. But if one of these freedoms is missing or incomplete, then the program controls the users and the proprietor controls the program.”

Without these freedoms, he argues, software becomes a tool of oppression.

“Non-free software is an injustice; non-free software should not exist; non-free software oppresses its users and therefore I won't use it,” says Stallman. “I don't have any. I go out of my way to ensure nobody does that to me, and also, because of my conscience, refuse to help to do that to other people.”

Spying on the user: Swindle, Shitbit and the Internet of Stings

Much of the proprietary software we use today, Stallman argues, contains malware. But not malware of the type your IT department is tasked to prevent, but code designed to harm the user’s privacy.

“Because the proprietors know they have control over users, they're attempting to mistreat users with that power,” he says. “They put in malicious functionalities. This is why the widely used proprietary programs are typically malware. And among other things, they often spy on their users.”

Here he’s taking a swipe at the major players: the makers of devices used by millions of us around the world.

“This is an example: this is Amazon's e-book reader, the Amazon Swindle. It transmits, from time-to-time, the name of the book being read and the page number to Amazon servers. If the user enters any notes, they're sent to Amazon too. Total Orwellian surveillance of the user,” he says. “I refuse to be oppressed this way: take that Swindle and step on it.”

But Amazon isn’t the only one collecting such intimate data.

“Lots of proprietary programs spy. Windows spies, Mac OS spies, iOS spies, Flash player spies. Thousands of apps spy on the user,” he says.

The proliferation of personal fitness trackers has, according to Stallman, amplified this.

Lots of proprietary programs spy. Windows spies, Mac OS spies, iOS spies, Flash player spies. Thousands of apps spy on the user

“The Shitbit: the device that keeps track of how you walk and sends the data to the company and then says 'would you like to buy this data back from me, data that's from you yourself? And who else can I sell it to?'” he says.

“The point is, that's an advanced form of spying. Whenever there's an app or a product that's tied to a particular server, that's something automatically that's going to shaft you.”

As the internet of things takes off, this looks set to greatly increase this type of data collection.

“The internet of things - well I call it the internet of stings - it's a way that those companies can get power over more things in your life, snoop on more things in your life and have total power,” he says. “And they start by saying its optional, and then your insurance company says 'if you use it we'll give you a discount', and slowly that morphs into 'if you don't use it we're going to charge you extra' and almost everybody feels compelled to say yes.

“And if we apply that kind of standard to consent to sex, it would be basically defining that there's always consent, isn't there? Which shows it’s the wrong standard to apply, and it's wrong here too.

“When people are systematically pressured into saying yes, they're not really saying yes.”

Software backdoors: Stalin’s dream?

One area is particularly concerned about is backdoors within software, that allow companies to remotely make changes to code or assets on people’s machines, and which, Stallman argues, allows them to “remotely attack the user”.

“The Amazon Swindle has a backdoor for erasing books. We saw this in 2009: Amazon remotely erased thousands of books, thousands of copies of the same book: it was 1984 by George Orwell,” he said. “So of course this stimulated a lot of criticism, so Amazon said it would never do this again, unless ordered to by the state. Right.

“Even if Amazon had meant that seriously, it would not be an adequate response. But Amazon didn't mean it seriously: it was just supposed to sound like a promise, supposed to take away momentum from the critics because a few years later Amazon went back to openly erasing books by force without even an order from the state.”

Then there’s Microsoft’s controversial update process, which is achieved through a universal backdoor in its operating system.

“Windows has had a universal backdoor since Windows XP: a universal backdoor means they can forcibly change the software at a distance,” he says. “It's a universal backdoor in the same sense that computers are a universal computing engine and can be programmed to do absolutely any nasty thing to the user.”

However, one of the biggest areas for concern for Stallman is smartphones, a device type that he refuses to own.

I call this Stalin's dream: this is what Stalin would have yearned for

“Portable phones, every portable phone has a universal backdoor,” he says. “So what is a mobile phone? It tracks a person's movements all the time, it has to do that in order to function, but the effect is that the phone company finds always where it is, and can localise it very precisely by triangulating with local towers.

“And with the backdoor they can convert it into a full-time listening device that can hear all the conversation in the room, even when it's not making any call, even when it’s supposed to be switched off.”

For Stallman, this is reality that the architects of the Soviet Union would have loved.

“I call this Stalin's dream: this is what Stalin would have yearned for,” he said. “But the point is: Stalin couldn't do that: it was too far-fetched even for him to dream of. But this is what's happening today.”

This might sound concerning, but there’s more: this is just what we know about. As all of this software is delivered as an executable, there is a considerable amount of software that little is known about, as researchers have been unable to discern exactly what it’s doing.

“Those programs are malware. But there are a lot of other proprietary programs that may or may not be malware, we don't know. We're unable to find out,” says Stallman.

“This is a situation that's a recipe for corruption, so of course power corrupts. The developers of proprietary software face this temptation, and a lot of them are corrupt, and the rest we don't know about.”