https://ideas.ted.com/why-an-insecure-internet-is-actually-in-tech-companies-best-interests/

Why an insecure internet is actually in tech companies’ best interests

Oct 26, 2018 / Bruce Schneier

Google, Facebook, Amazon and others make their profits in two main ways: by collecting as much data as possible from us and by controlling what we pay for, says online security expert Bruce Schneier. And what does this all depend on? A vulnerable internet.

Flaws in technology are not the only reason we have such an insecure internet. Another important reason — maybe even the main reason — is that the internet’s most powerful architects have manipulated the network to make it serve their own interests.

Everyone wants you to have security, except from them. Google is willing to give you security, as long as it can surveil you and use the information it collects to sell ads. Facebook offers you a similar deal: a secure social network, as long as it can monitor everything you do for marketing purposes. Harvard Business School professor Shoshana Zuboff calls this “surveillance capitalism,” and it’s the business model of the internet.

This surveillance is easy because computers do it naturally. Everything we do involving a computer creates a transaction record. This includes browsing the Internet, using — and just carrying — a cell phone, walking past a computerized sensor, or saying something in the same room as Amazon’s Alexa. Data is a byproduct of socializing that we do using computers — phone calls, emails, texts, Facebook chatter.

Our data used to be thrown away because its value was marginal and using it was difficult. Today, data storage is so cheap that all of it can be saved. This “big data” is fundamentally surveillance data, and it’s used by corporations, primarily to support the advertising model that underpins much of the internet. If you look at lists of the world’s most valuable companies from the past decade, you’ll find many that engage in surveillance capitalism: Alphabet (Google’s parent company), Facebook, Amazon and Microsoft.

> As long as companies buy, sell, trade and store our personal data, it’s at risk of being stolen. And as long as they use our data, we risk it being used against us.

Take a moment to consider who knows where your smartphone is, and therefore where you are. That list would include any apps you’ve given the permission to track your location — and some that track it by other means. Obvious ones are Google Maps and Apple Maps, but there are less obvious ones. For example, in 2013 researchers at Carnegie Mellon were surprised to discover that apps like

Angry Birds, Pandora Internet Radio and the Brightest Flashlight — yes, a flashlight app — also tracked users' locations. While much has changed in the intervening five years, with Apple again taking the lead here, it's still possible to give away lots of data without realizing it.

Surveillance companies know a lot about us. Google is probably the best example, as internet search is incredibly intimate. We never lie to search engines. Our interests and curiosities, hopes and fears, desires and sexual proclivities are all collected and saved by the companies that search the internet in our name.

To be clear: when I say "Google knows," I am not implying that the companies are sentient or conscious. Rather, I mean two specific things. One: Google's computers contain data that allow a person with access to it — authorized or unauthorized — to learn the facts, if they chose. Two: Google's algorithms can use this data to make inferences about us and perform automated tasks based on them.

The commercial Internet requires insecurity to operate at peak efficiency. As long as companies are free to gather as much data about us as they can, they will not sufficiently secure our systems. As long as they buy, sell, trade and store that data, it's at risk of being stolen. And as long as they use it, we risk it being used against us.

> Like feudal lords, tech companies like Amazon, Google and Facebook protect us from outside threats — and have surprisingly complete control over what we see and do.

Computers don't just allow us to be surveilled; they also allow us to be controlled. It's a new business model: forcing us to pay for features individually, use only particular accessories, or subscribe to products and services that we once purchased outright. And this kind of control relies on internet insecurity.

If you're a farmer who bought a tractor from John Deere, you may think that it is yours. Because tractors contain software — in essence, they're computers with an engine, wheels and a tiller — John Deere has moved from an ownership model to a licensing model. In 2015, John Deere told the copyright office that farmers receive "an implied license for the life of the vehicle to operate the vehicle." That license comes with all sorts of restrictions. Farmers have no right to repair or modify their tractors; instead, they have to use authorized diagnostic equipment, parts and repair facilities that John Deere has monopoly control over.

Apple maintains strict control over which apps are available in its store. It has strict rules about what it will and won't allow — no porn or games about child labor or human trafficking, but also no political apps. The latter rule meant Apple censored apps that tracked US drone strikes and apps containing "content that ridicules public figures," putting it in a position to be able to implement government censorship demands. And it's done so: in 2017, Apple removed security apps from its China store.

Normally, we wouldn't have a problem with a company making decisions about which products it carries. If Walmart won't sell music CDs with a parental warning advisory label, we can buy them elsewhere. But internet companies benefit from the network effect. One telephone is useless, two are marginally useful, but an entire network of phones is *very* useful. The same is true for email, the web, texts, Facebook, Instagram, etc. The more people use them, the more useful they are. And the more powerful the companies that control them become, the more control those companies can exert over you.

The situation on the internet is practically feudal. Some of us have pledged our allegiance to Google: we have Gmail accounts, we use Google Calendar and Google Docs and have Android phones. Others have pledged allegiance to Apple or to Microsoft. Or we buy music and e-books from Amazon, which keeps records of what we own and allows downloading to a Kindle, computer or phone. Like feudal lords, these companies protect us from outside threats, and they also have surprisingly complete control over what we can see and do.

> HP printers no longer let you use unauthorized ink cartridges. Tomorrow, HP might require you to use only authorized paper.

Companies are eyeing the internet of things in the same way. Philips wants its controller to be the central hub for your light bulbs and electronics. Amazon wants Alexa to be the central hub for your smart home. Both Apple and Google want their phones to be the singular device through which you control all your IoT devices. Everyone wants to be central, essential and in control of your world.

Battles for control of customers and users will heat up in the coming years. While the monopolistic positions of companies like Amazon, Google, Facebook and Comcast allow them to exert significant control over users, smaller, less obviously tech-based companies — like John Deere — are attempting to do the same.

This corporate power grab is all predicated on abusing the DMCA, the law that stymies the patching of software vulnerabilities. The DMCA was designed by the entertainment industry to protect copyright. But this pernicious law has given corporations the ability to enforce their commercial preferences. Because software is subject to copyright, protecting it with DRM copy protection software invokes the DMCA. The law makes it a crime to analyze and remove the copy protection, hence to analyze and modify the software.

John Deere enforces its prohibitions against farmers maintaining their own tractors by copy-protecting the tractors' computers. Keurig coffee makers are designed to use K-cup pods to make single servings of coffee. Because the machines use software to verify a code printed on each K-cup, Keurig can enforce exclusivity so only companies who pay Keurig can produce pods for its machines. HP printers no longer allow you to use unauthorized ink cartridges. Tomorrow, the company might require you to use only authorized paper or refuse to print copyrighted words you haven't paid for.

As the internet+ — I use this term because it goes way beyond the devices we associate with the internet of things — turns everything into computers, all that software will be covered by the DMCA. This same legal trick is used to tie peripherals to products, to limit consumers to buying authorized components, or only buy repair services from authorized dealers. This affects smartphones, thermostats, smart light bulbs, automobiles and medical implants.

> To ensure compliance with their restrictions, companies often monitor what their customers doing. Then they deny them access to that data.

Often, user control goes hand in hand with surveillance. In order to ensure compliance with the restrictions they demand from customers and users, companies often monitor what customers and users are doing. Then they deny the customers access to that data.

Customers are rebelling. People have been hacking their Toyota Priuses since 2004 to improve fuel efficiency, disable annoying warnings, get better diagnostic information out of the engine, modify engine performance, and access options only available in European and Japanese versions of the car. These hacks may void the warranty, but car manufacturers can't stop them. John Deere tractor owners have resorted to buying pirated firmware from Ukraine to repair their own tractors.

This isn't a black-and-white issue — we don't want people to have unfettered ability to hack their consumer devices. For example, thermostats deliberately have wide control limits. Changing the software to maintain the temperature can damage the heating system by forcing it to turn on and off too frequently. Similarly, that pirated tractor software from Ukraine may remove — accidentally or on purpose — the software that protects the transmission, causing it to fail. If John Deere is responsible for transmission repairs, that's a problem.

Similarly, we don't want people to hack their cars in ways that break emission control laws or their medical devices in ways that evade legal restrictions surrounding their use. Some people are hacking their insulin pumps to create an artificial pancreas — a device that measures their blood sugar levels and automatically delivers the proper doses of insulin on a continuous basis. Do we want to give them the ability to do that, or do we want to make sure only regulated manufacturers produce and sell those devices?

I'm not sure where the proper balance lies. As the internet+ permeates more of our lives, this conflict will play out everywhere. People will want access to data from their fitness trackers, appliances, home sensors, and vehicles, and they'll want it on their own terms, in formats they can use for their own purposes. They'll want to be able to modify those devices to add functionality.

Device manufacturers and governments will try to prevent enhanced capability — sometimes for profit, anticompetitive reasons or regulatory reasons, or because vendors didn't bother making the data or controls accessible. All of this reduces security. So in order for companies to control us in the ways they want, they will build systems that allow for remote control. More importantly, they'll build systems that assume the customer is the attacker and needs to be contained.

Excerpted from the new book Click Here to Kill Everybody: Security and Survival in a Hyper-connected World *by Bruce Schneier.*