Crossing the Digital Divide (v52)

"Check Point"

By Joseph Feigon for the Observer

This week's article was written by Quincy Larson of FreeCodeCamp.com. I often close my column with "Keep control of those things you can control". The topic today should serve as both a warning and sound advice.

On January 30th, Sidd Bikkannavar, a US-born scientist at NASA's Jet Propulsion Laboratory flew back to Houston, Texas from Santiago,Chile.

On his way through through the airport, Customs and Border Patrol agents pulled him aside. They searched him, then detained him in a room with a bunch of other people sleeping in cots. They eventually returned and said they'd release him if he told them the password to unlock his phone.

Bikkannavar explained that the phone belonged to NASA and had sensitive information on it, but his pleas fell on deaf ears. He eventually yielded and unlocked his phone. The agents left with his phone. Half an hour later, they returned, handed him his phone, and released him.

We're going to discuss the legality of all of this, and what likely happened during that 30 minutes where Bikkannavar's phone was unlocked and outside of his possession.

But before we do, take a moment to think about all the apps you have on your phone. Email? Facebook? Dropbox? Your browser? Signal? The history of everything you've ever done — everything you've ever searched, and everything you've ever said to anyone — is right there in those apps.

"We should treat personal electronic data with the same care and respect as weapons-grade plutonium — it is dangerous, long-lasting and once it has leaked there's no getting it back." — Cory Doctorow

How many potentially incriminating things do you have lying around your home? If you're like most people, the answer is probably zero. And yet police would need to go before a judge and establish probable cause before they could get a warrant to search your home. What we're seeing now is that anyone can be grabbed on their waythrough customs and forced to hand over the full contents of their digital life.

Companies like Elcomsoft make "forensic software" that can suck down all your photos, contacts — even passwords for your email and social media accounts — in a matter of minutes. Their customers include the police forces of various countries, militaries, and private security forces. They can use these tools to permanently archive everything there is to know about you. All they need is your unlocked phone.

“If one would give me six lines written by the hand of the most honest man, I would and something in them to have him hanged.” — Cardinal Richelieu in 1641

What’s the worst thing that could happen if the Customs and Border Patrol succeed in getting ahold of your unlocked phone? Well… Think of all of the people you’ve ever called or emailed, and all the people you’re connected with on Facebook and LinkedIn.What are the chances that one of them has committed a serious crime, or will do so in the future?

Have you ever taken a photo at a protest, bought a controversial book on Amazon, or vented about an encounter with a police officer to a loved one? That information is now part of your permanent record, and could be dragged out as evidence against you if you ever end up in court.

There’s a movement within government to make all data from all departments available to all staff at a local, state, and federal level. The more places your data ends up, the larger a hacker’s “attack surface” is — that is, the more vulnerable your data is. A security breach in a single police station in the middle of nowhere could result in your data ending up in the hands of hackers — and potentially used against you from the shadows — for the rest of your life.

Wait a second. What about my fourth and fifth amendment rights? Isn’t this illegal?

The fourth amendment protects you against unreasonable search and seizure. The fifth amendment protects you against self-incrimination. If a police officer were to stop you on the street of America and ask you to unlock your phone and give it to them, these amendments would give you strong legal ground for refusing to do so.

But unfortunately, the US border isn’t technically the US, and you don’t have either of these rights at the border.

It’s totally legal for a US Customs and Border Patrol officer to ask you to unlock your phone and hand it over to them. And they can detain you indefinitely if you don’t. Even if you’re an American citizen.

The border is technically outside of US jurisdiction, in a sort of legal no-man’s-land. You have very few rights there. Barring the use of “excessive force,” agents can do whatever they want to you.

So my advice is to just do whatever they tell you, to and get through customs and on into the US as quickly as you can.

The US isn’t the only country that does this.

It’s only a matter of time before downloading the contents of people’s phones becomes a standard procedure for entering every country.

This already happens in Canada. And you can bet that countries like China and Russia aren’t far behind.

“Never say anything in an electronic message that you wouldn’t want appearing, and attributed to you, in tomorrow morning’s front-page headline in the New York Times.” — Colonel David Russell, former head of DARPA’s Information Processing Techniques Office.

Since it’s illegal in most countries to profile individual travelers, customs officers will soon require everyone to do this.

The companies who make the software that downloads data from your phones are about to get a huge infusion of money from governments. Their software will get much faster — maybe requiring only a few seconds to download all of your most pertinent data from your phone.

If we do nothing to resist, pretty soon everyone will have to unlock their phone and hand it over to a customs agent while they’re getting their passport swiped.

Over time, this unparalleled intrusion into your personal privacy may come to feel as routine as taking off your shoes and putting them on a conveyer belt. And with this single new procedure, all the hard work that Apple andGoogle have invested in encrypting the data on your phone — and fighting for your privacy in court — will be a completely moot point. Governments will have succeeded in utterly circumventing decades of innovation in security and privacy protection. All by demanding you hand them the skeleton key to your life — your unlocked phone.

You can’t hand over a device that you don’t have.

When you travel internationally, you should leave your mobile phone and laptop at home. You can rent phones at most international airports that include data plans.

If you have family overseas, you can buy a second phone and laptop and leave them there at their home.

If you’re an employer, you can create a policy that your employees are not to bring devices with them during international travel. You can then issue them “loaner” laptops and phones once they enter thecountry.

Since most of our private data is stored in the cloud — and not onindividual devices — you could also reset your phone to its factory settings before boarding an international flight. This process will also delete the keys necessary to unencrypt any residual data on yourphone (iOS and Android fully encrypt your data). This way, you could bring your physical phone with you, then reinstall apps and re-authenticate with them once you’ve arrived. If you’re asked to hand over your unlocked phone at the border, there won’t be any personal data on it. All your data will be safe behind the worldclass security that Facebook, Google, Apple, Signal, and all these other companies use.

Is all this inconvenient? Absolutely. But it’s the only sane course of action when you consider the gravity of your data falling into the wrong hands.

If you bother locking your doors at night, you should bother securing your phone’s data during international travel.

This may upset Customs and Border Patrol agents, who are probably smart enough to realize that 85% of Americans now have smart phones, and probably 100% of the Americans who travel internationally have smart phones. They may choose to detain you anyway, and force you to give them passwords to various accounts manually. But there's no easy way for them to know which services you use and which services you don't use, or whether you have multiple accounts.

We live in an era of mass surveillance, where governments around the world are passing terrifying new anti-privacy laws every year.

> "Those who are willing to surrender their freedom for security have always demanded that if they give up their full freedom it should also be taken from those not prepared to do so." — Friedrich Hayek

With a lot of hard work on our part, enlightenment will triumph. Privacy will be restored. And we will beat back the current climate of fear that's confusing people into unnecessarily giving up their rights. In the meantime, follow the Boy Scouts of America Motto: always be prepared. The next time you plan to cross a border, leave your phone at home.