Clavister White Paper Series: No Back Doors

The Unknown Unknowns Dilemma:

What You Don't Know Can, In Fact, Hurt You

Governments, led by the US example, are creating more and more surveillance strategies into personal and business information using backdoors, peering into the cloud and upstream data gathering. This white paper tells you what you need to know to protect your customers and business reputation.

The digital age has brought us into one of the most conflicted inflections of the human experience. How can we live in such a vast free environment of unfettered information while at the same time having that freedom under attack from malicious actors? And for the purposes of this white paper, the most powerful entity in our lives—the state—becomes an ubiquitous and quiet threat that creates a security threat of unknown scope and depth.

It's similar to the once cryptic, Ayn Rayn inspired quote by former US Defense Secretary Donald Rumsfeld that points to the quandary of state surveillance and deep intrusion into our digital networks, lives and business continuity. "There are known knowns. These are things we know that we know. There are known unknowns. That is to say, there are things that we know we don't know. But there are also unknown unknowns. There are things we don't know we don't know." Indeed, since Edward Snowden, we now know that intrusion of our devices was massive and shook the world. Phones could be switched on to capture sound and audio without our consent or knowledge that the device was even turned on; individual movements were being collected in big data sieves that could use the data for both terror fighting but also dissident surveillance such as Pegasus, the Israeli surveillance software used by UAE and other states to track NGOs, journalists and those considered critical of their regimes. Through Snowden's whistleblowing, PRISM which revealed access to Americans' Google and Yahoo accounts could be ordered by the US government, XKeyscore which could access any internet or phone record from a laptop and of course the Tailored Access Operations" (TAO) unit that has paved the way for cyberwarfare. This was the opening shot in the war on deep intrusion and it sent a political and societal thunderclap throughout our world.

There is another revelation that Snowden exposed and one that has caused an unease to businesses in the same way as the initial reports caused for individual privacy. It's also one that—after those initial outrages—not only has continued but is increasing. So much so that we're in Known Unknowns: ie that we know something is happening but its scope and breadth evade us.

The Known Unknowns

What was exposed in the Snowden whistle blowing dump in relation to technology infrastructure revealed a shocking truth. That—on top of the privacy intrusion that used the internet and telecom networks—a strategy was devised that would penetrate the very physical architecture of our digital world. Under a programme that started in the 1970s called BLARNEY with further iterations called OAKSTAR, FAIRVIEW and STORMBREW. Under the heading of "passive" or "upstream" collection the concept was to capture data that travelled across fiber-optic cables and the gateways that direct global communications traffic. One of the techniques to achieve this penetration was to pay the vendors, software companies and network providers a stipend to have access to their technology, to their hardware. To their customers. The black budget—revealed in 2013 by Washington Post investigative reporting and freedom of information documents gathered by lawsuits—shows that the US pays hundreds of millions of dollars to these firms including security vendors to plant backdoors that governments officials, should they choose, can use to access data from companies and individuals. The budget documents obtained by The Post list $65.96 million for BLARNEY, $94.74 million for FAIRVIEW, $46.04 million for STORMBREW and $9.41 million for OAKSTAR. It is unclear why the total of these four programs amounts to less than the overall budget of $278 million.

"There are known knowns. These are things we know that we know. There are known unknowns. That is to say, there are things that we know we don't know. But there are also unknown unknowns. There are things we don't know we don't know."

Former US Defense Secretary Donald Rumsfeld

"It turns surveillance into a revenue stream, and that's not the way it's supposed to work," said Marc Rotenberg, executive director of the Electronic Privacy Information Center, a Washington-based research and advocacy group. "The fact that the government is paying money to telephone companies to turn over information that they are compelled to turn over is very troubling," he stated in the Washington Post piece. The PRISM programme or the "downstream" component of the NSA strategy had more FISA court overview. With the infrastructure programme the payments, which ostensibly were for the costs of fulfilling FISA requests and buying equipment to fulfill the programme objectives plus profit, could easily create the incentive for the vendors to 'look the other way' as data gathering happened or create plausible denial scenarios that keeps investors, board members and managers compliant.

With the US clearly in the lead for this kind of programme, a recent memo by the so called 'Five Star' partners (US, UK, Canada, Australia and New Zealand), a group of countries allied to fight criminality using surveillance, have issued a memo that calls on a new, more sweeping backdoors policy to be implemented that tackles one of the most serious threats to their mission: end-to-end encryption and VPN tunneling. The Five Star have issued the memo that providers "create customized solutions, tailored to their individual system architectures that are capable of meeting lawful access requirements." This kind of backdoor access would allow each government access to encrypted call and message data on their citizens. If the companies don't voluntarily allow access, the nations threatened to push through new legislation that would compel their help.

"Should governments continue to encounter impediments to lawful access to information necessary to aid the protection of the citizens of our countries, we may pursue technological, enforcement, legislative or other measures to achieve lawful access solutions," states the memo.

Last but not least, the recent Clarifying Lawful Overseas Use of Data ("CLOUD") Act of 2018 that launched in the US has becoming a new known unknown in that its powers seem incredibly wide ranging. Targeted at cloud providers, its goal is to have access to data in other countries that is stored in a US cloud provider's platform. That means Azure, AWS, Google and other US

based providers would have to open their customer's data to government requests or risk legal wrath. And while some legal minds argue that this gives more clarity to countries trying to comply to these requests and even challenge them, especially under the Stored Communications Act (SCA), privacy defenders and those warning of state level industrial espionage (Electronic Frontier Foundation (EFF) and 23 other civil liberties organisations, including the American Civil Liberties Union (ACLU) to name a few) warn of negative consequences.

1. The Act expressly provides that U.S. law-enforcement orders issued under the Stored Communications Act (SCA) may reach certain data located in other countries.
2. The Act also allows certain foreign governments to enter into new bilateral agreements with the United States that will prequalify them to make foreign law-enforcement requests directly to U.S. service providers, rather than via the U.S. government under a mutual legal assistance treaty. This should streamline compliance with foreign law-en forcement requests.
3. The Act formalizes the process for companies to challenge a law enforcement request.
4. The Act imposes certain limits and restrictions on law enforcement requests to address privacy and civil liberty concerns.

Boiled down, the CLOUD Act has two major components. First, it empowers US law enforcement to compel US companies to hand over data that is stored outside the US. This means law enforcers can serve a search warrant for a company's data and the company will have to comply, even if that data is stored in a foreign jurisdiction.

Second, the Act creates new venues for cross-border data transfer called 'executive agreements', which will be unilaterally decided by the US executive branch. The executive agreements will be between the US and foreign governments that wish to reciprocate. Once agreements are approved, foreign governments will have a new mechanism for obtaining data directly from US companies, as long as that data does not belong to a US person or a person living inside the US.

"The CLOUD Act bypasses the current system in place for when law enforcement agencies want access to data stored across their borders," says David Ruiz, a policy analyst at the EFF in the Financier Worldwide. "That system, governed by MLA treaties, typically requires law enforcement agencies to follow both the data protection laws of their country and the data protection laws of the country where the data is stored. Under the CLOUD Act, foreign governments could ask US companies for US-stored data, as long as that data does not belong to a US person or a person living in the US, without needing to abide by US data privacy laws. This is wrong."

"It turns surveillance into a revenue stream, and that's not the way it's supposed to work. The fact that the government is paying money to telephone companies to turn over information that they are compelled to turn over is very troubling."

Marc Rotenberg, executive director of the Electronic Privacy Information Center, a Washington-based research and advocacy group

Unknown Unknowns

The most telling and worrying category of the backdoor threat is simply all the things we don't know. Of course there is a legal verneer that says that this ability to look at our data has checks and balances, is not akin to the Stasi rifling through our homes and offices at will. But is that true? How do we know that a deeper level of government, who are exempted from the judicial process, takes precedent. Surely acts of national security, of war and peace can be used to

circumvent all those legal structures. And as Eternal Blue taught us, weapons are out there that fall into the wrong hands and create panic. Willingly/unwillingly, knowingly/ unknowingly, there must be things we can do to address this creeping intrusion into the public trust.

It is the question of the entities that we can only suspect are tapping into these technologies and strategies—countries and organizations, above the service and below—that reveal the greatest existential threat. Oppressive regimes using surveillance to spy on journalists, political dissent, alternative lifestyle groups to silence them. We know all too well what such tools can give to the darker sides of our nature. And like any asymmetrical weapon, this one can wreak havoc on a scale we're simply unable to fathom.

"The CLOUD Act bypasses the current system in place for when law enforcement agencies want access to data stored across their borders,"

says David Ruiz, a policy analyst at the EFF in the Financier Worldwide.

Solutions

One solution is for security or data infrastructure providers to not accept a golden handshake of monetary compensation to participate in this ecosystem of spying. It is morally wrong, especially to the businesses and individuals who don't know this situation is happening and have not given consent. In an era of privacy protection laws and concerns, the technology industry itself should create these standards of transparency.

A second solution is for consumers to be aware of the backdoors dilemma and choose to work with providers that have taken a clear stance against willing backdoor collusion. Clavister, an independent cybersecurity firm based in the North of Sweden, has called on all technology companies to commit to a no backdoors pledge, as legally binding as possible, to break this complicit chain and alert consumers to their rights and responsibilities.

Last but not least, countries themselves—like Sweden who has a Pirate political party and safeguards for data privacy that exceed other countries—should create safe harbours for datacenters, cloud providers and technology companies who wish to be shielded from large state legal directives. They should also require that clients and citizens are fully aware of data privacy in the same way that eco produce has certification and agencies verifying its compliance. Taken together, and with a strong hand that pushes back on these intrusions rather than simply being the one that opens the door to let these murky state actors inspect data, the public and businesses can get the safety they require without having to forfeit the rights that we hold dear.

Sam Colman
Director of Marketing and
Corporate Communications

Find out more on our Security by Sweden page
https://www.clavister.com/vikings

CONNECT . PROTECT

Clavister AB, Sjögatan 6 J, SE-891 60 Örnsköldsvik, Sweden
■ Phone: +46 (0)660 29 92 00 ■ Fax: +46 (0)660 122 50 ■ Web: www.clavister.com