An Open Letter to Fight for Digital Security and Privacy

In the past, law enforcement agencies have been able to read the contents of suspects' devices and wiretap their communications with relative ease. The recent rise of technologies that encrypt data when it is stored or transmitted has made law enforcement's job much harder. With their old techniques rendered useless, they have started to force the device and software vendors to implant "back doors" or special access to the encrypted data. These back doors undermine all security protections and put all users at risk. Currently, there is no current legislation that protects encryption or prevents law enforcement from demanding back doors. We, the security and privacy community, need your help to get this issue on our lawmakers' radars. Once the politicians are focused on the issue, we will help them understand why back doors are dangerous using by explaining the technical details.

Encryption is vital to ensuring the security and privacy of individuals. But what is encryption and how does it work? Encryption is the encoding of information and messages in a way that only the intended recipient can properly decode the message and read its contents. Most modern smartphones encrypt all data stored on the device by default, and an increasing number of messaging services encrypt messages before they are sent out so they are secure in flight.

In the context of encryption, allowing someone to read the actual contents of an encrypted message is known as trusting them. Best security practices say one should establish trust in as few people as possible, preferably only the intended recipient. On the web, this is accomplished via a complex certificate exchange process which ensures that websites are who they say they are. On a single device, this involves trusting just yourself, since the encryption key is derived from your password, stored on the device, and never shared assuming only you know the password. Allowing the government to plant back doors requires users to place trust in the government as well as any other parties. Trusting more people inherently reduces security and increases the likelihood of a breach because there are more potential points of failure. Additionally, there is often little to no verification that the correct party is accessing the back door. This means that malicious actors can easily bypass security protections by reverse engineering the back door's access mechanism. This is very dangerous because it could allow criminals and nation-state threat actors to gain unchecked access to countless devices.

Privacy experts fear that the US Government could use these new capabilities for more than just law enforcement. The ability to simply read data off devices and decrypt network traffic can be used to perform large scale surveillance. This was already attempted by the government multiple times and is being implemented in China. Proponents of digital privacy claim that the government does not have the authority to snoop on citizens at this level. The Fourth Amendment of the Bill of Rights guarantees protection against search and seizure without a warrant. If the government starts intercepting communications of citizens without obtaining warrants for all of them, this could be considered a violation of Fourth Amendment rights.

As mentioned above, there are no laws which explicitly prevent law enforcement from forcing companies to install back doors. However, it is very difficult to challenge the law enforcement agencies' practices in court because they manipulate the law to their advantage. The first law they bend for protection is the Wiretap Act. The Wiretap Act states that if law

enforcement has a subpoena to intercept a suspect's communications, then they can request access to "all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively." The piece most often exploited in the context of back doors is the ability to request technical assistance. Law enforcement is abusing this law in order to justify forcing companies to implant back doors into their products.

The second law being abused by law enforcement is the All Writs Act. In the Supreme Court case of United States v. New York Telephone Co. in 1977, the Telephone Company resisted an FBI request to install special equipment in their infrastructure. The company claimed that the order did not authorize the FBI to make this request and that they should have used a subpoena under the provisions of the Wiretap Act instead of the All Writs Act. The Supreme Court ruled that an All Writs Act based order requires companies to comply with requests as long as they are deemed to require minimal effort. Law enforcement is manipulating the lack of specific definition of "minimal effort" in order to force the installation of back doors into software and devices. This is a blatant misuse and abuse of power by law enforcement.

The final law that law enforcement is taking advantage of is the Foreign Intelligence Surveillance Act (FISA). The act allows the Attorney General and the Director of National Intelligence to create written requests that require service providers to "immediately provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition." The power granted by FISA is mostly the same as the Wiretap Act. One key difference is that companies must comply with the order secretly. This allows law enforcement to force back doors into technology, while also keeping their existence a secret. At first glance, this may seem more secure than requesting a back door via the Wiretap or All Writs Acts. However, simply hiding the existence of these back doors does not improve security in any concrete way. In the security field, this is known as security by obscurity since it seeks to protect the back doors by making them more confusing to find. As described above, a determined or skilled enough threat actor would work through the obscurity and find the back door anyway. When law enforcement uses FISA in this way, they are not only abusing their power, but they are causing a false sense of security as well.

In order to put a stop to this deliberate abuse of power by law enforcement, legislators must pass new laws that more clearly define the limits of any requests made to aid in investigations. This new legislation will help modernize policy with new technology in mind, while also protecting the privacy and security of the individual and the nation. Legislators will need to learn about the dangers of back doors from security and privacy experts through roundtables and hearings. We, the security and privacy community, are more than willing to engage with legislative bodies in this way and in order to provide technical expertise in our fields. This exchange of ideas will ensure that any new laws align with best practices. However, none of this will happen if lawmakers aren't focused on improving policy in this area. We need normal citizens to write letters to the politicians that represent them indicating interest in the back door issue. These lawmakers were elected to fight for the needs of the citizens in their districts, and these letters will show lawmakers that constituents care about security and privacy. They need to understand that all new legislation has to be guided by technical principles in order to best protect citizens, and collaboration between lawmakers and security and privacy experts is the only way to achieve this.

Works Cited

[1] C. Soghoian, "Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era," *Journal on Telecommunications & High Technology Law*, vol. 8, no. 2, pp. 359–424, 2010.