HEARING BEFORE
THE UNITED STATES SENATE JUDICIARY COMMITTEE

December 10, 2019

Testimony of Matt Tait

Chairman Graham, Ranking Member Feinstein, members of the Committee, thank you for inviting me to this important hearing.

For as long as this country has existed, society has always struggled to maintain a balance between individuals' rights to privacy versus the rights of victims of crime to obtain justice through law-enforcements' ability to collect evidence and prosecute the crimes committed against them.

Time and again, the inevitable progress of technology shifts this balance in one direction or the other, and we are here again today because technology has once again shifted this balance.

Encryption makes us undoubtedly safer online from hackers and foreign government surveillance. Without it, the Internet would not be the thriving hub of commerce that it is today. Encryption has made it possible to communicate securely with one another, to build businesses online, and enables us to access global communities and shared interests that previously were hard to access. The Internet and the technology market today is as it is precisely because encryption enables us to operate online securely.

As with all technologies, encryption comes with inevitable collateral externalities, in this case to law-enforcement. It is right that we ask hard questions about what we can do to mitigate these collaterals without undermining the huge benefits to society that encryption gives us all.

We should not be coy: encryption does affect law-enforcement in practically all domains, from counter-terrorism, financial crimes, countering child abuse, as well as ordinary device searches for local law-enforcement. And given the sheer scale and complexity of these domains, it is hardly surprising that the conversation around encryption needs some work itself to decipher.

As I understand it, encryption meaningfully hinders law-enforcement in three key areas that need to be taken separately: *device searches*, *wiretaps*, and so-called "cyber tips" whereby distribution of child abuse material can be detected and investigated. Perhaps surprisingly, the way encryption relates to these domains is not similar to one another, and the approaches for technology companies, law-enforcement, and regulators to address these collaterals have surprisingly little overlap.

The first of these three domains is *ordinary device searches* which is impacted by *device encryption*. Device encryption entangles a users' files with the passcode of the user in order to prevent unauthorized extraction of those files. This has the collateral effect of preventing law-enforcement from searching devices that have been physically seized during an arrest or property search. If the owner cannot enter their passcode, perhaps because they are dead at the scene of a crime, either as a victim or perpetrator, the device provides no alternative mechanism to access the content of the device.

The second of these domains is *traditional wiretaps* between two individuals known to law-enforcement to be planning or committing a major crime. This is impacted by *end-to-end communications encryption* ("E2E encryption"), which hides all content, but not all metadata, of the conversation taking place, so that not even the communications provider can see it.

The third domain is what law-enforcement calls "cyber tips" in the context of detecting when child abuse imagery is shared over a communications platform. At the moment, many technology companies voluntarily scan shared images against a huge database of known child abuse material, and alert law-enforcement if a match is discovered. Although this domain is very different to traditional wiretaps, it is also affected by *end-to-end communications encryption*, because without access to the content being transmitted, technology companies are more limited in their ability to scan content for abuse material.

Each of these three domains impact law-enforcement in quite different ways, and the ability of technology companies, law-enforcement, or regulators to counteract these collaterals are surprisingly different.

For example, the use of zero-day vulnerabilities has, in effect, become the accepted default mechanism for law-enforcement and intelligence agencies to conduct wiretaps on end-to-end encrypted platforms. A few months ago, a recent hacking campaign attributed to China made use of iPhone zero-day vulnerabilities to access, among other things, the content of WhatsApp and iMessage communications from targeted devices.

Zero-day vulnerabilities are not cheap, but at least for now, wiretaps via hacking remain an attractive, practical, and proportionate method for federal law-enforcement to conduct wiretaps without the need for proactive regulation or help from technology vendors.

The so-called "cyber-tips" are a harder challenge to bridge. Here the use of zero-day vulnerabilities to break into substantively all devices and scan for abuse material would clearly not be safe or proportionate. But other approaches do exist that do not require the alteration or removal of end-to-end encryption. For example, technology vendors can scan for abuse images as they are sent and received on the device itself rather than as it traverses the communications platform.

I do not wish to trivialize the difficulty of this task; it is harder than it sounds, and something technology companies can and should do more research on.

In short, options exist for both conducting wiretaps and retaining "cyber tips" without the need for altering or regulating end-to-end encryption. These options are not easy, to be sure, but they exist.

Uniquely among the problem domains, only device encryption, which thwarts device searches, would be amenable to a "front door" access mechanism. This is because device searches can be predicated on the knowledge, if not consent, of the owner, and the technology to do so can be built around law-enforcement's physical access to the device. Because these factors are not available in the context of wiretaps, it will always be dangerous to extrapolate technological access mechanisms for *device searches* to wiretaps or end-to-end encryption generally.

In summary, encryption remains an important tool for enabling the Internet to operate as the hub of commerce and communication that is increasingly the center of all our lives. There are collateral externalities to law-enforcement investigations, but many of these externalities can be mitigated entirely without reference to the encryption itself.

The path forward is not easy; technology always comes with new and unexpected collateral risks. But with a bit of work, some from technology vendors to mitigate harms of their platform, some from law-enforcement up-skilling their workforce to deal with new threats, we can take advantage of the technical benefits of pervasive encryption while minimizing most or all of the collateral externalities that it might impose on the rest of society.

Thank you, Mr. Chairman. I appreciate the opportunity to be here today, and I look forward to answering the Committee’s questions.

# # # #