LIBERTY
GROUP
VENTURES

Prepared Testimony of
Kiersten E. Todt

Before the
House Committee on Energy and
Commerce, Subcommittee on
Communications and Technology

Room 2322 Rayburn House Office Building
10AM
Tuesday, June 13, 2017

I. Introduction

Good afternoon Chairman Blackburn and Ranking Member Doyle. Thank you for the opportunity to present my testimony on the promotion of security in wireless technology. I am currently the Managing Partner of Liberty Group Ventures and a Resident Scholar in Washington, DC at the University of Pittsburgh Institute for Cyber Law, Policy, and Security. I also serve on the Federal Advisory Board of Lookout, Inc. I most recently served, from March 2016 to March 2017, as the Executive Director of the Presidential Commission on Enhancing National Cybersecurity. This independent, bipartisan Commission was tasked by then-President Obama to assess the state of our nation's cybersecurity; this group of twelve Commissioners, four of whom were recommended by leaders of both parties in the Senate and the House of Representatives, was charged with developing actionable recommendations for growing and securing the digital economy. The Commission completed its report on December 1, 2016 and the Chair of the Commission and I presented the key recommendations to then-President Obama. The report includes six imperatives, 16 recommendations, and 53 action items.

I appreciate this Subcommittee's awareness of the need to focus on the security of wireless and mobile technology. In a world where "first to market" overrides "secure to market" and every enterprise – industry, government, and/or individual – is seeking to make operations move more quickly and be more convenient, addressing the security of these innovations is critical and absolutely necessary. In response to the questions posed by this hearing, my testimony will primarily focus on mobile security and address the growing threat environment around interdependencies and the Internet of Things, which I will refer to as IoT.

II. Mobile Security

In this age of data breaches, mobile devices, which are highly portable, constantly connected to various networks, and are being used to access cloud services across personal and enterprise computing, are an attack vector that cannot be ignored. Mobile devices are increasingly targeted for access to sensitive information or financial gain. Mobility should not be at odds with security. As an individual, you should have the freedom to communicate, shop, bank, etc. without worry. And at work, IT/security professionals should be able to secure the sensitive data accessible on their employees' mobile devices, yet still enable business to run as usual.

The growing adoption of mobile in the enterprise has allowed for increased flexibility and productivity. However, due to this shift, mobile devices have rapidly become ground zero for a wide spectrum of risks that includes malicious targeted attacks to devices and network connections, a range of malware families, non-compliant apps that leak data, and vulnerabilities in device operating systems or apps.

The reality is that cloud and mobile adoption in the enterprise is just beginning. Analysts have predicted that mobility-related initiatives will grow from 25 percent of IT budgets to

40 percent in the next 3 years. Therefore, now is the time to implement mobile security. Mobile devices are part of every supply chain – in your home and in your office. We need to treat mobile devices as an endpoint priority equal to, if not more important than, traditional endpoints, such as desktops and laptops.

Mobile devices have become much more than communication devices. They are the access point to our work and personal lives. Today, many individuals bank and make purchases from their devices; they collaborate on sensitive work documents, and they monitor their personal health data. I recently had bloodwork done and was told the only way I could access the results was by downloading an app onto my smartphone. Additionally, with the rise of two-factor-authentication -- an important step in ensuring the security of your accounts, but not the ultimate solution -- the smartphone has become even more important than the password. A compromised device could hand over to an attacker an authentication code -- and thus access to an individual's most personal information, as well as any work-related sensitive information.

Apple has done an excellent job building products with security in mind. They also take tremendous care to ensure that malicious apps do not end up in the App Store. However, when it comes to security, particularly for enterprises or government agencies, it's advisable to exercise a defense-in-depth strategy. All products have latent security vulnerabilities that could be exploited by bad actors. Many users ignore security policies and download apps from unofficial sources. Users can also be tricked into compromising the integrity of their device by installing a malicious profile when connecting to public WiFi networks. Otherwise benign apps can have behaviors (such as accessing data and/or sending it to unknown servers) that violate a company or organization's security policies. To mitigate these risks, an enterprise should have many layers of security protecting the sensitive data that matters most.

Currently, it takes enormous effort to reverse engineer and remediate a cyberattack and only minimal effort for attackers to modify their code and infrastructure to successfully evade detection. As we are often reminded, defense has to be right always – an attacker only has to be right once. An industry over-reliance on signatures and behavioral analysis detection models has much to do with the problem. Signatures can't scale with the pace of malicious software development and they routinely miss advanced attacks. Behavioral analysis models tend to produce more false positives, creating excessive noise that can cause organizations to lose or overlook important signals surfaced by the detection model.

There are currently more than two billion mobile devices worldwide, with more than 4 million apps in app stores being constantly updated, and thousands of device types and OS versions generating hundreds of billions of data points. Effective security for the mobile world analyzes potential mobile threats not in the context of a single server, a single device, or a single application, but in the context of global mobile devices and code.

Some enterprises wonder why they haven't heard of an enterprise data breach resulting from an attack on mobile devices. It's not that the threats aren't there, it's that most organizations don't have visibility into them. According to a recent Ponemon study, 67% of the Global 2000 reported that a data breach occurred as a result of employees using mobile devices to access the company's sensitive and confidential information. In the userbase of Lookout, a leading mobile security company, over the course of six months, they found that on average, 47 out of 1000 Android enterprise devices encountered an app-based threat, including spyware, data exfiltrating trojans, and root enablers that compromise the integrity of the device.

Last summer, Lookout and Citizen Lab detected the Pegasus spyware. Pegasus is a sophisticated form of spyware that was being used against a political activist in the UAE, and possibly other targeted individuals around the world. Pegasus took advantage of three iOS zero day vulnerabilities to take complete control of a device. The attack was capable of getting messages, calls, emails, logs, etc. from apps including Facetime, Facebook, Line, Mail.Ru, KakaoTalk, Calendar, WeChat, SS, Tango, WhatsApp, Viber, Skype, Gmail, and more. This threat represents the first time anyone has seen a remote jailbreak of an Apple device in the wild and shows us that highly resourced actors see the mobile platform as a fertile target for gathering information about targets, particularly high risk groups like activists, and regularly exploit the mobile environment for this purpose.

Mobile Security and the Federal Government

Historically, government agencies have been quite restrictive about the use of mobile devices in the workplace. However, in a survey conducted by Lookout, the government worker finds ways around the rules. In this survey of government workers, 40 percent of employees at agencies with rules prohibiting personal smartphone use at work say the rules have little to no impact on their behavior.

Perhaps because agencies have recognized that mobility is happening with or without their permission, we are beginning to see a shift towards prioritizing mobility initiatives in the federal government. A year ago, mobile wasn't on the top 10 priorities for DHS, now it's in the top 3. We also know that DISA is working on making it possible for employees to access Google Play and the Apple App Store on their mobile devices. As agencies recognize the benefits of mobility and embrace it, they must build in proper security from the beginning.

In general, all government agencies should recognize the risk of spyware, other data exfiltrating trojans, network attacks, operating system and app vulnerabilities, and apps that are otherwise benign but may leak sensitive data. The bottom line is that smartphones are essentially a supercomputer — and today, most have absolutely no security software on them.

The federal government should establish mobile as a core pillar of the security infrastructure. For example, it may be worth considering how mobile could be integrated into the DHS reauthorization bill, which was released last week. Mandates or policies stipulating that mobile devices must have an agent on the device that does predictive analytics, could make a difference in how government views mobile security. Additionally, as is the case across all enterprises, public and private, senior leadership needs to be educated on mobile security to appreciate that while they may have deployed mobile tools, they haven't deployed mobile security. I would like to take this opportunity to commend John Ramsey, the CISO of the U.S. House of Representatives for recently purchasing 8000 licenses for mobile security technology (from Lookout), which he is in the process of deploying. This example is one where Congress is ahead of the Executive branch in implementing a cybersecurity best practice; I encourage this Committee, perhaps in collaboration with the House Homeland Security Committee, to hold a hearing on and to examine how federal agencies can do a better job to defend against mobile security risks.

Federal agencies must also work to stay ahead of the unintentional mobile security threats of human behavior. This issue is, of course, one that cuts across all elements of cybersecurity. The human is the greatest security threat – and a cyber naïve human is an even greater threat. Today, federal agencies have no insight into the devices and applications accessing their data. So, they have no way to get ahead of potential security issues -- whether they come from malicious actors or unassuming employees. Most agencies today do have policies with regard to the use of mobile devices, however, most will also tell you that they aren't effective because they have no way to enforce them.

The Commission on Enhancing National Cybersecurity highlighted the mobile work environment as the environment of today and the future. Many government agencies are not paying sufficient attention to the mobile threat environment, even as we continue to introduce new devices, systems and platforms that introduce a proliferation of interdependencies into networks and thus new vulnerabilities. As the report states, the concept of the classic security perimeter is largely obsolete. Additionally, the government needs to secure all Department and Agency IT assets, including IoT and other network-connected devices, such as smartphones. With mobile access to sensitive data on the rise and digital data becoming increasingly blurred between physical and cyber assets, strong government-industry collaboration that prioritizes the new frontiers of cyber attacks is imperative to our nation's cybersecurity.

III. The Growing Threat Environment

As we appreciate the growing threat event, and for the purposes of this hearing, the challenges presented by wireless and mobile security, we appreciate that the increase in interdependencies, across critical infrastructure and non-critical infrastructure, caused by the proliferation of IoT devices is a growing challenge. There are a broad set of recommendations and actions that can be taken to address this threat – depending on which aspect of the challenge one is examining.

Our interconnections and interdependencies are becoming more complex and now extend well beyond critical infrastructure (CI). These interconnections reduce the importance of the CI label because, by association, all dependencies may be critical – as we saw with the Dyn/Mirai attack last fall. As these linkages grow, so does the need to consider their associated risks. This convergence, combined with increased cybersecurity awareness, creates a unique opportunity to change our current approach to protect the digital economy.

We need to recognize that neither the government nor the private sector can capably protect systems and networks without close and extensive cooperation. Critical infrastructure owners and operators deserve clearer guidance and a set of common understandings on how government responsibilities, capabilities, and authorities can lead to better collaboration and joint efforts in protecting cyberspace.

Today, it is widely assumed and expected that the private sector is responsible for defending itself in cyberspace regardless of the enemy, scale of attack, or the type of capabilities needed to protect against the attack. That makes cyberspace the only domain where we asked companies to defend themselves. This assumption is problematic. The government is – and should remain – the only organization with the responsibility and, in most cases, the capacity to effectively respond to large-scale malicious or harmful activity in cyberspace caused by nation-states – but, with the assistance of an in coordination with the private sector. Our current structure does not set up this type of collaboration.

One initial step that needs to be taken to develop this type of collaboration is the development of an entity, similar to the President's Intelligence Advisory Board, which convenes senior leaders from government and industry to address cybersecurity issues. This entity would focus on pre-event planning. Government does incident response well. But, government does not effectively work and collaborate with industry, routinely, before events occur. Taking a page out of the Pentagon playbook, government and industry should train and exercise together on a regular basis. We continue to develop several initiatives that focus on information sharing – a term that is so overused it has lost its meaning. But, information sharing is not a destination – information sharing is a byproduct of relationships and trust that is built between and among entities. If we are going to truly secure the digital economy and the increased innovations around wireless and mobile technologies, industry and government must have a vehicle for collaboration, which creates value for both. Through this process, government and industry should address cybersecurity through a risk management approach – to ensure an enterprise's approach to cybersecurity takes into full account prioritized assets, resources, and risk appetite.

IV. Conclusion

Companies, large and small, as well as government agencies and other organizations, now have more tools at their disposal to assess and take action to better understand and respond to cyber risks. Once organizations are enabled to better manage those risks, they can make informed decisions about how to apply scarce resources to yield the greatest value. We now recognize mobile security as one of the greatest risks affecting all enterprises. And, we therefore need to treat mobile devices as an endpoint priority equal to, if not more important than, traditional endpoints, such as desktops and laptops.

America prides itself on fostering the individual entrepreneur, the independent and creative spirit, and the competitor who stands above all others. When it comes to tackling the diverse and broad array of cybersecurity challenges, we need those qualities –but we need joint efforts, collaboration, and cooperation even more. Government and industry each have different strengths and limitations in their cybersecurity capabilities. Mechanisms that clearly define public-private collaboration, joint planning, and coordinated response before, during, and after an event are critical and must be effectively developed. We must have complete awareness of how technologies, especially mobile, are being used and deployed in order to secure those technologies most effectively.

No technology comes without societal consequences. The challenge is to ensure that the positive impacts far outweigh the negative ones and that the necessary trade-offs are managed judiciously. In doing so, we can and must manage and significantly lower cybersecurity risks, while protecting privacy and civil liberties. We must also put in place forward-thinking, coherent policies, developed in a transparent process that enable our institutions and our individuals to innovate and take advantage of the opportunities created by new technology – specifically, for the purposes of this hearing, wireless and mobile technologies.

Thank you for the opportunity to testify in front of you today. I look forward to answering your questions.