# Data Protection, Law Enforcement and the Global Digital Economy

**Testimony of Jon Potter**
**President, Application Developers Alliance**

U.S. House of Representatives
Subcommittee on Information Technology
Committee on Government Oversight and Reform
Hearing on "Encryption Technology and Possible U.S. Policy Responses"

April 29, 2015

Chairman Hurd, Ranking Member Kelly and Members of the Subcommittee:

Consumers want their personal data protected and businesses want their confidential data protected. Cyberhackers and data thieves are a constant threat. For several years law enforcement and consumer protection officials have encouraged the data protection marketplace and used enforcement tools to insist and demand that consumer data be protected. And responding appropriately to marketplace and government forces, app developers and our digital industry partners regularly provide and promote encryption tools to ensure that consumers' personal information and private communications remain private.

Thank you for inviting me to share with you today the challenges that app developers and our digital industry partners will face if we try to both protect privacy *and* provide privacy-breaching back doors to the government. Others will testify about the technological impossibility of this task. I will speak to the resulting legal and investment uncertainty, consumer mistrust, and business turbulence. And when this hearing and the longer debate concludes, I urge Congress to remain committed to protecting Americans' privacy, empowering encryption solutions that can eradicate cyberhacking and data theft, and upholding traditional American values that require law enforcement to abide by the Constitution.

The Application Developers Alliance (the "Alliance") was founded in January 2012 to support app developers as entrepreneurs, innovators, and creators. Alliance membership includes more than 200 companies and an additional 36,000 individuals.

On behalf of the app industry and our innovative, entrepreneurial members, I ask you to consider the following:

1. The Federal Trade Commission (FTC), State Attorneys General, the FBI, privacy advocates and consumers are correct: protecting data while using it to build exciting new products and services is unquestionably good for businesses and consumers. The entire app ecosystem is committed to both data innovation and data protection.
2. By challenging the use of encryption and sending a conflicting message about data protection, law enforcement is introducing doubt about what is expected or perhaps required of app developers and digital businesses. This creates uncertainty for all, but especially for risk-averse, resource-constrained startups and small innovators. Investors and customers often flee from uncertainty, and though talented app developers can code virtually anything, they should not have to choose between conflicting government demands – particularly of the gravity of privacy and data security.
3. The app marketplace is international and nearly every app wants to be global. If apps are required to provide back doors to the U.S. government, then many other governments will require their own access key or their own back doors, and still other governments will cite these back doors as evidence of non-compliance with their national privacy laws. Instead of enjoying global digital opportunities, apps will be buffeted by conflicting laws that force unpleasant choices while imposing financial and legal risk. App developers and their customers will have to choose between compliance and market access.
4. Privacy-breaching back doors make apps inherently less secure and less trustworthy. By providing access to one or more governments, the developer is creating a vulnerability that can be exploited by hackers and thieves.
5. For 15 consecutive years, identity theft has been the #1 consumer complaint to the FTC. Data protection prevents cybercrime and identity theft, and encryption is the best data protection tool we know. Encryption proponents are not simply favoring privacy and civil liberties, we also favor crime prevention – the essential result of strong data protection.

**Today's Privacy vs. Law Enforcement Debate is Not New, But It Is Different**

Like many policy debates spawned by technological advances, today's encryption debate is like a new cover version of an old song. America's privacy vs. law enforcement debate really began in the 1700s, when colonists resisted British soldiers who were permitted unfettered access to homes, businesses, and property. The Fourth Amendment – prohibiting unreasonable searches and seizures – is the direct result of colonists' umbrage and is the foundation of 200 years of America's civilian government.

More than 200 years after the Bill of Rights was ratified, innovators were building and commercializing the first wave of digital networks and privacy-focused companies were deploying the first generation of encryption technologies. At that time America's national security and law enforcement agencies expressed urgent concern about hostile foreign entities having access to that era's best encryption technology. In response, Congress approved the Communications Assistance for Law Enforcement Act ("CALEA") and thereby required companies to build law enforcement back doors into broadband and Voice-Over-IP networks and related equipment. Despite guaranteeing law enforcement access to communications, Congress sought to ensure that legal process would be followed prior to that access being utilized. Moreover, Congress recognized the importance of data security and included explicit protection for encryption and encrypted communications.

Today's debate is different, however, in part because circumstances have changed but also because law enforcement goals have transformed.

One significant new circumstance is that businesses and consumers are more technologically savvy and are smarter about data protection. Weekly reports about leading companies being hacked by organized cybercriminals, combined with so many consumers' personal experiences with identity theft, have propelled a market for security and encryption products. Identity theft has been the top consumer complaint to the FTC for fifteen consecutive years, and that trend is driving commercial activity.

Consumers and businesses are also responding to recent revelations of widespread, untargeted, bulk surveillance by national security and law enforcement agencies. This activity, including seemingly willful disdain for proper legal process, has made citizens justifiably skeptical of law enforcement promises that unfettered access to digital networks will be utilized judiciously. International governments are similarly provoked, and are requiring U.S. companies

to ensure that international consumers' (including businesses) data is protected, including against the U.S. government.

Encryption is no longer a niche market. In 1994, there were few digital products and services and the market for encryption was small and specialized. But today on my phone I have a traditional mobile telephone service as well as Viber, WhatsApp, Google Hangouts and Skype. Each of these apps, the operating system on my phone, the software in each network access point and the networks themselves may incorporate encryption so that my private conversations remain private. This privacy is also critical for business and enterprise apps to ensure privacy of, for example, trade secrets, financial and health care data.

As a result of this global focus on trust and security, many businesses are bundling encryption with products and services and are investing to improve those offerings. Venture capitalists and institutional investors are betting heavily on secure trust-based business models, while computer scientists are building better systems that provide more privacy and security value – developments eagerly awaited by businesses and consumers concerned about cyberthieves and identity theft.

Yet, against this trend in favor of privacy and security, the FBI and law enforcement are attacking and seeking vulnerabilities in encryption technologies that Congress has explicitly protected. Law enforcement has an obvious and substantial interest in prosecuting crime and protecting people, but creating encryption vulnerabilities that will enable more identity theft and cause more consumer harm is not the right solution.

**The Implications of Today's Privacy v. Law Enforcement Debate Are More Significant and Potentially Much More Severe**

In light of the ubiquity of digital products and services, and the magnitude of cybercrime and identity theft, it is perplexing that the FBI and law enforcement are disparaging the very large, substantial and determined encryption market that it has encouraged. This effort cuts against prevailing wisdom and sends confusing, unhelpful suggestions to app developers, and to the publishers and enterprises that developers work with.

First, developers whipsawed by the government's mixed messages may be paralyzed in their development cycle. As developers, investors and customers ask which government agency is in charge and whether data protection is really a government-approved value, the marketplace

can freeze up. If this uncertainty continues for too long then lawyers will have to help developers make a difficult and perhaps pyrrhic decision: which federal mandate should I follow and which one should I ignore?

The Subcommittee should appreciate the magnitude of mixed messages developers have received. Over the course of several years virtually every government law enforcement and consumer protection agency has sung from the encryption and data protection hymnal.

- The FTC advises consumers that "[e]ncryption is the key to keeping your personal information secure online," and consistently requires app developers to use "reasonable" data security practices, including encryption, to protect consumers' information from hackers and data thieves.
- California Attorney General Kamala Harris recommends that app developers "transmit user data securely, using encryption" and endorses legislation "requiring encryption to protect personal information in transit."
- The FBI recommended organizations "encrypt data so the hacker can't read it."
- President Obama's Review Group on Intelligence and Communications Technologies recommended that the U.S. Government promote national security by "fully supporting and not undermining" encryption standards and generally available commercial encryption, and "supporting efforts to encourage the greater use of encryption technology for data in transit, at rest, in the cloud, and in storage."
- And in February President Obama personally called on industry to protect Americans' privacy and civil liberties, and proclaimed himself "a strong believer in strong encryption…. there's no scenario in which we don't want really strong encryption."

Against this backdrop, industry responded. Hardware manufacturers are selling encrypted Blackphones. Companies such as Apple, Google and Yahoo are embedding encryption into their software and operating systems. Snapchat, Yik Yak and SpiderOak are offering encrypted consumer solutions, and industries such as banking, health care, transportation and manufacturing are extremely focused on secure, encrypted solutions.

Additionally, nearly every app is pursuing international customers and every contract developer seeks international clients. Thus, it is important that Congress consider other

countries' reactions to U.S. digital policy and how other countries' policies could create challenges to American digital services or America's global interests.

By demanding unfettered access to encrypted products and services, the FBI is putting American digital companies' international opportunities at risk. European and South American policymakers have virulently criticized U.S. Government collection of European citizens' and leaders' communications data, and many have demanded that U.S. companies provide assurances that their products and services are not susceptible to U.S. Government hacking. Leading European policymakers have repeatedly urged more robust European consumer privacy laws, stating forthrightly that this is intended to harm U.S. digital services and advantage European services. Mandating privacy-breaching back doors increases the risk that international governments will cite U.S. companies' non-compliance with privacy laws to justify banning American apps from doing business in their country. Compounding this problem are governments – for example Russia, China and some in South America – that are choosing to only do business with companies based in their own country.

The App Developers Alliance is a global organization and our European and American members are equally optimistic about our industry, consumer adoption and economic opportunity. None of our members – anywhere in the world – desire a trade war that divides the global Internet and global opportunity into smaller subsets of national markets. But if Congress requires U.S. companies to provide open backdoors for FBI access, it should anticipate European policymakers to respond emphatically. Mandatory privacy-breaching back doors will instigate trade wars and exacerbate international business challenges.

Third, mandatory back doors diminish consumer trust and create challenges for apps and all digital businesses. In addition to government risk, app developers will face marketplace challenges if forced to provide privacy-breaching back doors to law enforcement. Our customers – in the United States and abroad – expect their communications to be private and secure when purchasing or using apps. Since our sector's inception just a decade ago, developers have prioritized the security and handling of their customers' data because they know that good data stewardship is critical to business success. Enabling governments to access data without proper legal process risks undermining the customer trust that app developers worked hard to obtain.

Congress should also anticipate that governments worldwide will demand their own back door key or separate back doors for their own security and law enforcement interests. This will

increase further the risk that consumer and business data could be compromised. Larger consumer app publishers might have the resources to build multiple back doors and might have enough consumer trust to withstand the associated scrutiny, but startups and resource-limited small innovators will be challenged to find resources to build multiple back doors, and will also have greater trust problems than established competitors. Of course, all apps not complying with other governments' demands could easily be locked out of those markets.

As a purely technological matter any opening in security creates a vulnerable access point for hackers, thieves, and foreign governments to exploit. While the FBI would have us believe that law enforcement alone will be privy to our sensitive data, history demonstrates that bad actors will always be ahead of the curve and find an avenue to manipulate those openings. As one well-regarded cryptographer said – "you can't build a backdoor that only the good guys can walk through."

Currently, consumers read about data breaches on an almost daily basis. Though the market is demanding tighter security measures, there are only two types of companies in the world: those that have been breached and those that do not know they have been breached. Consumers expect businesses to respond to these breaches and many have bolstered their security features, sometimes through encryption. Requiring companies to build in a back door undermines consumers' and businesses' desires to secure data in storage, in transit, and across the supply chain. End-to-end encryption is the only way to secure user data from all outside forces while simultaneously giving consumers greater control of their data.

Fourth, forcing holes in encryption harms startups and small innovators the most. Many – perhaps most – of the small companies that are Alliance members lack the resources to create country-specific access points for law enforcement agencies around the world. It is relatively easy to build a back door, but difficult to build a back door that only certain people – the right people – can access. While the U.S. government is pleading to tech companies "let us in," they simultaneously warn companies to keep hackers and other countries out. Because building a back door that is slightly ajar is technically challenging and very expensive, it is extremely difficult for large companies, let alone startups, to meet these conflicting demands. App developers and startups already must overcome significant cost hurdles before products get to market, and any regulatory inconsistency or redundancy is one burden too many.

While situations may occasionally justify law enforcement and national security agencies' access to our cell phones, such as a missing child, or matter of exigency, our statutes are filled with multiple, well-established, legal methods to access this data. Congress should insist that U.S. law enforcement and national security agencies utilize these processes before mandating back doors into apps, digital products and digital services.

* * * * *

In closing, I urge Congress to remember that encryption technologies are a market response to consumer demands, business needs, and U.S. and international governments' widespread calls to protect consumer data,. When an app developer builds a thriving business model around privacy, security and consumer trust, only to be told the FBI wants your products to be secure, but not too secure, this disrupts the marketplace. It is bad for innovation, bad for business and bad for consumers. It is only good for hackers and cyberthieves who prey on private consumer data and commercially sensitive data.

Americans correctly demand that their personal data is secure. Just as importantly, businesses deserve clear and consistent messages from our government to ensure a stable marketplace. I look forward to your questions and the Alliance looks forward to working with Congress on this important issue.