2016 LEGISLATIVE PRIORITIES TO PROTECT DIGITAL PROPERTY

The federal government's all-encompassing mass surveillance through warrantless seizures and searches of all citizens' digital information must end. Pervasive electronic monitoring, interception and other seizures of electronic information intrude on individual liberty and property, and violate the Constitution's due process, property, privacy, expression and associational rights. Data Foundry, Golden Frog and Giganews support the following legislative initiatives in 2016:

Update ECPA

- The House Judiciary Committee will mark-up HR 699 on April 13, 2016 amidst efforts to secure amendments that threaten the integrity and purpose of the bill. The Committee should pass the bill without significant change. Although non-substantive technical edits and minor changes may be acceptable, Golden Frog opposes broader proposals, including significant definitional changes to current law that will create uncertainty and might lead to unintended outcomes in the courts.
- ECPA sets the rules for when police and the government can read our email, look at our photos and access other content stored in the cloud. The law passed in 1986 does not take proper account of current technology or the way citizens use digital information (property) today.
- Under current law government and law enforcement officials can access personal communications and documents in remote storage in the cloud with merely a subpoena, meaning no prior consideration from a judge is necessary. This massive vulnerability in privacy rights opens the door for government snooping and complete disregard for our constitutional liberties.

Cybersecurity and Privacy Principles

- Government should tend to its own information security before it tries to regulate or dictate the methods and means by which businesses operate in this area.
- Government should observe and require due process and use proper legal standards for mandated business disclosure of information about other businesses and individuals.
- Government should limit its gathering and retention of sensitive information to only that which is necessary; share sensitive information with other agencies only when appropriate; and keep sensitive information only for so long as it is needed for the purpose for which it was gathered.
- Effective cybersecurity measures require robust encryption. Strong, defensive encryption technologies are integral to securing cyber infrastructure. Cybersecurity measures that employ robust encryption must be ubiquitously deployed throughout sensitive government and private computer systems. The government should encourage further industry development of encryption technologies and resist policies that would compromise the integrity of encryption systems that protect against cyber threats.

Protect American Citizens' and Small Businesses' Ability to Use Encryption Services

- Congress must pass legislation protecting citizens' and small businesses' right to individually encrypt their digital information while stored in their devices (cell phones, computers, portable drives), in transit through communications networks, and in cloud storage.
- Encryption is not new. It is merely a form of cyphering, which has been used for centuries. The American Revolution may not have been successful without the extensive recourse to cyphering our founders used to ensure secure communications.
- Secure encryption should be equally available to small businesses and individuals as a means to protect their property and their privacy.

Contact: Andy MacFarlane andymac@datafoundry.com 512.684.9414

2016 LEGISLATIVE PRIORITIES TO PROTECT DIGITAL PROPERTY

- Encryption is not a threat to national security and it should not draw suspicion from the FBI, NSA or other authorities. User encryption and other efforts to maintain privacy and property cannot, standing alone, form the basis for reasonable suspicion, probable cause or even special attention. Encryption is now merely how users demonstrate an objective expectation of privacy. Encryption is a proper tool for people to secure their property from digital theft and appropriation, and it is protected by the First, Fourth, Fifth, Ninth, Tenth and Fourteenth Amendments. Businesses encrypt confidential and proprietary information such as trade secrets and customer data.
- Encryption is a form of self-defense. In the same way that firearms are synonymous with the Second Amendment and protecting oneself and one's property, using encryption to protect your data is how one protects his or her digital self and digital property. Privacy conscious citizens use it to protect their private digital information from hackers, and prevent government and corporate intrusion. Encryption protects digital property, just like a lock on a door.

Ban Government-Mandated Backdoors Into Americans' Cellphones and Computers

- Congress should pass legislation that prohibits government mandates to build backdoors or security vulnerabilities into U.S. software and electronics.
- The information we generate and store is our property and we have a reasonable expectation of privacy. Compelled and involuntary "backdoor" access via a service or device provider on a pre- or post-sale basis constitutes a taking, because it destroys the bundle of property rights, including (a) the right to exercise sole dominion and (b) to exclude others.
- Any government agency that asks Congress to draft legislation enabling backdoors is misleading legislators. Cryptography experts will tell you there is no such thing as a secure backdoor. Backdoors are based on knowledge. Whoever knows the secret knock can open the secret door, but the door doesn't know who is knocking. Secrets inevitably become known outside their secret circle. If the NSA or FBI (or anyone else) has a backdoor into all encryption technologies, they will become the target of every spy agency in the world and scores of malicious hackers.

Proceed to Address Communications Content Collection by Amending Section 702 and Replacing Executive Order 12333 with Congressionally-passed Statutory Controls

- Congress should (1) significantly scale back Section 702 to limit mass content collection, (2) better control and restrict access to the collected information, (3) do more by way of limitations on use, sharing between non national security agencies and (4) impose a deadline for information destruction. FISA. Section 702 and Executive Order 12333 must be revised to better protect privacy and eliminate mass surveillance and information collection.
- U.S. intelligence agencies have operated without effective oversight for too long, and the unaccountable, non-transparent, massive surveillance programs can no longer continue unchecked.
- The wholesale interception and storage of users' content that is occurring without a warrant or demonstration of probable cause under Section 702 and 12333 must end. The government's claim that it can lawfully seize all communications content and then obtain a particularized authorization to "search" does not withstand constitutional muster. The seizure itself is a taking without due process, in violation of the Fifth Amendment, and violates the Fourth Amendment as well.

Contact: Andy MacFarlane andymac@datafoundry.com 512.684.9414