Andrew D. Macfarlane *Director-Governmental Affairs*
P: +1 512-684-9414 | C: +1 512-789-8601
andymac@goldenfrog.com | www.goldenfrog.com

Golden Frog's Legislative Priorities to

PROTECT AMERICANS' ONLINE PRIVACY

The government's ongoing efforts to pervasively monitor citizens' through electronic monitoring, interception and by gathering digital information intrude on individual liberty and property, and violate the Constitution's due process, property, privacy, expression and associational rights. Congress must act before we turn into a full-blown state of dragnet surveillance.

Golden Frog supports the following legislative initiatives in 2015:

Protect American Citizens' ability to Use Encryption Services

- Congress must pass legislation protecting users' right to individually encrypt their digital information while stored in their devices (cell phones, computers, portable drives), while in transit over the Internet, and while in cloud storage.
- 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. Such efforts are merely today's digital expression of a demonstration of an objective expectation of privacy, akin to putting a padlock on a storage room door. In the same way that firearms are synonymous with the 2nd Amendment and protecting oneself and one's property, using encryption to protect your data should be synonymous with protecting your digital self and your digital property.
- Encryption is a form of self-defense. Privacy conscious citizens use it to protect their Internet communications and private information from hackers, as well as government and corporate intrusion. Businesses encrypt confidential and proprietary information such as trade secrets and customer data. Encryption protects digital property, just like a lock on a door.

Ban Government-Mandated Backdoors Into Americans' Cellphones and Computers

- The information we generate and store is our property and we have a reasonable expectation of privacy. Compelled unencrypted "backdoor" access via a service provider would constitute a taking, since it destroys the property owner's 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. The problem with secrets is that they eventually become known outside their secret circle. If the NSA or FBI (or anyone else) has a backdoor into

golden frog™

Andrew D. Macfarlane *Director-Governmental Affairs*
P: +1 512-684-9414 | C: +1 512-789-8601
andymac@goldenfrog.com | www.goldenfrog.com

all encryption technologies, they will become the target of every spy agency and malicious hacker in the world.

- Congress should pass legislation that prohibits government mandates to build backdoors or security vulnerabilities into U.S. software and electronics.

Limit the Reauthorization of the USA PATRIOT Act, Curb NSA Surveillance & Pass a Meaningful Version of the USA Freedom Act

- 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.
- With expiration of the Patriot Act's authorities for bulk data collection looming, Congress must institute the reforms necessary to restore the balance and limitations within which Congress and the public intended for our intelligence apparatus to operate. It's time to demonstrate to citizens worldwide that they can trust that their private data is safe in the hands of American digital service providers.
- There must be a clear, strong, and effective end to bulk collection practices under the USA PATRIOT Act, including under the Section 215 records authority and the Section 214 authority regarding pen registers and trap & trace devices. Any collection that does occur under those authorities should have appropriate safeguards in place to protect privacy and users' rights.
- The bill must contain transparency and accountability mechanisms in place for government and company reporting, as well as an appropriate declassification regime for Foreign Intelligence Surveillance Court decisions.
- Not much attention has been paid to the government's bulk collection of actual content that is allegedly based on Section 702. Congress must end the wholesale interception and storage of users' content that is occurring without an actual warrant or demonstration of probable cause. 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.
- The government separately claims authority to engage in bulk meta-data and content collection under Executive Order 12333. Congress must end this executive branch overreach and constrain the President's extra-statutory power-grab.
- The federal government's all-encompassing mass surveillance through warrantless seizures and searches of all citizens' communications, including content, must end. Congress should significantly scale back FISA, and overrule Executive Order 12333 by replacing it with statutory authorizations/controls.

Update ECPA

- 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.
- ECPA has remained unchanged since it was passed in 1986 despite incredible technological advances of recent decades. This has left our communications open to unwarranted government intrusion.
- As the law is currently written, 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 Fourth Amendment rights.
- Last Congress, great strides were made to update ECPA for the digital age but reform did not come to fruition. Congress must act this year to appropriately protect Americans' privacy and property so that our rights on the Internet will finally be equivalent to the physical world.