GOLDEN FROG & DATA FOUNDRY'S LEGISLATIVE PRIVACY PROPOSALS

Texas sets the standard for protecting privacy rights. Last session, Texas became the first state in the country to statutorily require government officials to obtain a warrant from a judge to search the content of citizens' electronic communications. The U.S. Supreme Court's landmark *Riley v. California*, 134 S.Ct. 999 (2014) decision held that cell phone contents are protected by the Fourth Amendment, but Texas had preceded them by four months with the Court of Criminal Appeals' decision in *State v. Granville*, 423 S.W.3d 399 (Tex.Crim.App., 2014). The 2015 legislative session presents an opportunity for Texas to continue to lead the nation in protecting liberty by enacting additional commonsense safeguards for Texans' fundamental privacy rights.

Data Foundry provides the following list of potential privacy bills that would uphold the intent of the Fourth Amendment[1] and protect citizens' Fifth Amendment property rights[2] to their personal data, but not unduly restrict law enforcement.

1. **Warrant Requirement for Cell Phone Geolocation Data**

   In the Supreme Court's 2012 *U.S. v. Jones* decision, 132 S.Ct. 945 (2012), five justices determined that the electronic records of Americans' locations are protected by the Fourth Amendment. This decision required that police obtain a warrant to track Americans by installing GPS devices on their cars, but did not directly address the GPS devices that we carry in our pockets. Since the *U.S. v. Jones* decision, at least four states have required that police first obtain a warrant before seizing location records from cell phone companies.

   In 2013, HB 1608 was introduced to protect Texan's location data with a warrant standard. This bill's language was inserted into SB 1052, which passed the House by an overwhelming 124-5 vote. However, SB 1052 did not come up for a vote in the Senate before the session ended. HB 1608 included acceptable language providing several important exceptions that addressed legitimate law enforcement concerns. This bill would be an appropriate vehicle to reintroduce the effort to protect cell phone location data in 2015. Alternatively, the American Legislation Exchange Committee (ALEC) has put forth a model electronic privacy bill that requires warrants for geolocation records.[3]

[1] See also Tex. Const. Art. I, § 9.
[2] See also Tex. Const. Art. I, § 19.
[3] Electronic Data Privacy Act, § 4. Available at http://www.alec.org/model-legislation/electronic-data-privacy-protection-act/.

2. Warrant Requirement for Devices that Locate Cell Phones

The use of "Stingray" devices[4] has become another common way for law enforcement to intercept and monitor citizens' communications and determine their location. These devices mimic cell phone towers and trick nearby phones into announcing their identity and location to the Stingray. The owner of the cell phone has no idea that law enforcement is communicating with his cell phone and obtaining its location or content.

The warrantless and indiscriminate use of Stingrays infringes upon citizens' expectations of privacy in their location. A majority of the Supreme Court has determined location information to be protected by the Fourth Amendment. Therefore, law enforcement officers should only use Stingray devices after demonstrating probable cause to a judge and obtaining a particularized warrant. Furthermore, the warrantless use of stingrays should be considered an unconstitutional trespass upon a citizen's personal property because the Stingray transmits radio waves into a person's cell phone without his or her consent. When the Stingray is in full active mode it carries out a full intercept of all communications content as well, which means it is also taking each affected individual's private property – their "digital information" which could include not only private facts but also legally privileged content such as attorney-client, priest-penitent, spousal, medical, or confidential business trade-secret information.

Establishing a warrant requirement for the use of Stingrays by law enforcement officers would also have the ancillary benefit of immunizing officers that are acting pursuant to a warrant from prosecution under the Texas anti-hacking statute. Currently, any officer using a stingray could be charged with violating section 33.02(a) of the Texas Penal Code, which prohibits "knowingly access[ing] a computer, computer network, or computer system without the effective consent of the owner."

3. Warrant Requirement for Location Monitoring of Texans

State and local governmental authorities can monitor Texans' locations using tools other than Stingrays and seizing geolocation information. For instance, the RFID chips that Texans carry on their persons or in their cars can be monitored by creating a network of RFID scanners. In 2013, HB 101 sought to prohibit the use of RFID chips to monitor Texas public school students. Biometric monitoring of individuals is also now feasible and public video cameras could be used to locate and track individuals in public automatically.

By establishing a warrant requirement, the legislature would prevent the use of such technologies on a comprehensive and indiscriminate basis. Texans should not be

[4] "Stingray" is a trade name for one of the most popular devices. The more general name for all similar devices is "IMSI catcher."

tracked by their government wherever they go in public and, to do so, would almost certainly constitute a violation of the Constitution. A warrant requirement will ensure that these tools are used only against specific individuals and only after a showing of probable cause to a judge, which is in keeping with the Fourth Amendment.

4. Protections for Private Data Collected by State and Local Governments

State and local government entities collect vast amounts of information about Texans. The Committee should use the interim charge process to investigate the scope of private data that Texans surrender and the policies in place to protect that information. Important questions about the security of Texans' private information have never been fully addressed. For instance, which state and local entities retain biometric or RFID information? What is the purpose of gathering this information? What steps are taken to maintain security of the data? How long is this information retained? Is the information shared with other government or non-government entities? If so, under what conditions? The same questions should be asked about cell phone location data and other potentially invasive records. Once the Committee gathers these answers and understands the scope of data collection currently taking place, bills that protect this information can be proposed and studied.

5. Protections for Encrypted Data

Encryption is a form of self-defense. Encryption is the "Second Amendment of the Internet," so to speak. Texans use encryption 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. In recent years, the National Security Agency has deemed the use of encryption tools to be *per se* suspicious. The NSA collects and works to decrypt Texans' encrypted Internet communications. Recently, Data Foundry has seen evidence that broadband Internet providers are blocking encrypted communications.

A bill that protects the use encryption would advance Texans' right to defend their private information and communications from others. This bill would add the decryption of Texans' encrypted data to the list of forbidden "computer crimes" in section 33.02 of the Texas Penal Code, which is Texas's anti-hacking statute. This bill would also require law enforcement to obtain a probable cause-based warrant from a judge prior to decrypting a Texan's encrypted information. Lastly, this bill would also establish that no negative legal inferences, in either civil or criminal cases, may be drawn against a Texan that uses encryption. For example, merely encrypting one's communications should never, in and of itself, be deemed sufficient to establish probable cause.

6. Warrant Requirement for Compelled Disclosure of Passwords

Data Foundry proposes that Texans' passwords be protected from government compulsion with a warrant requirement. This would further strengthen and clarify the existing warrant requirement for content. Such a provision was proposed by ALEC in its Electronic Data Privacy Protection Act model bill, which states:

> [A] Government Entity may not compel a User or Geolocation Information Service to provide a passkey, password, key code, to any Geolocation Information or Electronic Device without a valid search warrant issued by a duly authorized judge or justice using state warrant procedures.

Requiring warrants for the compelled disclosure of passwords – and the information that they protect – would prevent the warrantless search and seizure of private data under threat of arrest. It would provide at least some protection against efforts to require a person to provide testimonial facts that could potentially be incriminating.[5] Withholding passwords without a judicial warrant would not constitute resisting a search (Tex. Penal Code § 38.03), interference with public duties (*Id.* § 38.15), hindering prosecution (*Id.* § 38.05), or any other state crime. Consensual disclosure of passwords should otherwise be permitted, but Texans' right to keep their sensitive information private must be protected.

7. Protections for Data Collected by License Plate Scanners

License plate scanners on police cars are being used in many jurisdictions to automate queries for outstanding warrants, lapsed insurance, unpaid traffic tickets, or other violations. These systems, however, have also raised serious privacy concerns. Through public information requests, citizens have learned that some localities are compiling databases with the photos and location of each scan. This information can be used to create a picture of a citizen's life. If it is paired with other surveillance technologies it becomes exponentially more invasive.

To address the public's concerns, the legislature should enact a bill that protects Texans' fundamental privacy rights by strictly limiting the time that such information can be saved and prohibiting sharing with third parties. Such a law should not categorically ban the use of license plate scanners because they are simply automating a legitimate police function. Citizens accept that when they drive, they share the road with police and those police can perform a license plate search on their vehicle. The potential harm from license plate scanners arises from the increase in the number of searches these systems can perform and the creation of databases that compile location information.

[5] See Tex. Const. Art. I, § 10.

Data Foundry proposes that records created by license plate scans that did not produce any legally actionable information be deleted within one week of creation. This allows the scanners to still be used for their intended function, as well as a short investigative period, but limits the potential for abuse that arises from maintaining the information indefinitely. A seven day limit also falls safely within the 28 day period at issue in *U.S. v. Jones*.

8. <u>Amend the Data Breach Notification Law to Include Government Hacking</u>

Nearly all states, including Texas, require that businesses notify their customers or the public at large when they have suffered a breach of their computer systems that has exposed customers' personal information. Without these laws, businesses would have little incentive to secure private data or disclose its theft. In Texas, businesses that fail to report a data breach are subject to civil penalties up to $250,000. Yet after it was reported in 2013 that the NSA hacked the networks of two large Internet service and email providers, neither company reported the breach to their millions of Texas users.[6] This may be because these companies interpret government hacking to not be an "unauthorized" acquisition of computerized data and, therefore, not a "breach of system security" that requires reporting under the statute.[7]

Data Foundry proposes that the Texas data breach notification statute be amended to explicitly state that the law applies equally to hacking performed at the hands of the government. It is just as important (if not more) for Texans to be informed that their government has stolen their private electronic information without due process as it is when the theft was perpetrated by an individual hacker. Public disclosure of such events promotes government accountability and the rule of law. Such an amendment to the current law would require the addition of only one sentence to section 521.053 of the Texas Penal Code:

> A "breach of system security" includes the acquisition of computerized data by federal, state and local government entities acting without a warrant that meets the standards of the Fourth Amendment.

Each of these proposed privacy bills would uphold Texans' fundamental rights and further establish Texas as the nation's leader in electronic privacy. This distinction is good for business because it creates a climate in which companies seek out Texas as a location to locate their data and operations. Protecting Texans' liberty is one of the most important responsibilities of the Texas legislature and Data Foundry looks forward to working with the State Affairs Committee to make 2015 a year of action for electronic privacy.

---

[6] Barton Gellman & Ashkan Soltani, *NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say*, Washington Post (Oct. 30, 2013). Available at http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

[7] See Tex. Penal Code § 521.053(a).