TASK FORCE ON DIGITAL INFORMATION PRIVACY

DATE October 1, 2014

TO Joint Corporations, Elections & Political Subdivisions Committee

FROM Task Force on Digital Information Privacy

SUBJECT Task Force Recommendations

The Wyoming Task Force on Digital Information Privacy held three meetings on the topic of digitally stored private information. Specifically, the legislation creating the Task Force, 2014 Senate File 91 (attached), required the Task Force to consider: (1) who is the owner of digitally stored private information; (2) what are the threats to consumers from the intentional or inadvertent compromise of digitally stored private information; (3) how consumers may be protected from those harms; (4) judicial decisions and federal statutes affecting privacy protection of digitally stored individual information; (5) ways to ensure that privacy protections are enforced; and (6) other issues the Task Force considers useful in encouraging appropriate safeguards for the privacy of digitally stored information.

1. Owner of digitally stored private information

The Task Force heard from the Wyoming Department of Enterprise Technology Services (ETS) and various state agencies as to the owner of digitally stored private information. Flint Waters, Director, ETS, explained how the department oversees the secure transfer of personal data from one agency to another. Mr. Waters explained that ETS did not own or control any data collected by the various agencies. Several state agencies, such as the Department of Workforce Services and the Wyoming Community College Commission, testified to the collection, storing and protection of personal information. The testimony suggested that the individual owned the personal information collected. However, it appeared unlikely that the individual had the right to correct any inaccurate personal data held by an agency.

2. Threats to consumers from the intentional or inadvertent compromise of personal data

The Task Force heard testimony from Adi Kamdar, Activist, Electronic Frontier Foundation, on the harms to consumers from the intentional or inadvertent compromise of personal data. In particular, Mr. Kamdar discussed situations where companies with large troves of sensitive personal information have suffered data breaches and put consumers at risk of identity theft.

Under current Wyoming law, identity theft occurs when one willfully obtains the personal identifying information of another person, alone or in conjunction with any other information, without permission and uses that information for an unlawful purpose. W.S. 6-3-901(a). Personal identifying information for

purposes of identity theft includes "the name, address, telephone number, driver's license number, social security number, place of employment, employee identification number, tribal identification card number, mother's maiden name, demand deposit account number, savings account number, or credit card number of an individual person." W.S. 6-3-901(b).

3. Consumer protection

As to how consumers might be protected from the intentional or inadvertent compromise of digitally stored information, the Task Force heard from Pam Greenberg, Senior Fellow, National Conference of State Legislatures. Ms. Greenberg discussed state security breach notification laws for the unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal identifying information. Ms. Greenberg noted that state security breach laws differed on the definition of personal information, notification requirements and enforcement and remedy provisions.

Under current Wyoming law, personal identifying information for purposes of security breach means "the first name or first initial and last name of a person in combination with" one or more specified data elements such as social security number; driver's license number; or account number, credit card number or debit card number in combination with any security code, access code or password that would allow access to a financial account of the person. W.S. 40-12-501(a)(vii). When personal identifying information is compromised or reasonably likely to be compromised, a business must notify affected consumers and provide a toll-free number. W.S. 40-12-502(a) and (e). The attorney general may bring an action to address violations of the state security breach notification statute. W.S. 40-12-502(f).

4. Relevant judicial decisions and federal statutes

The Task Force heard testimony from Robert Sprague, Associate Professor, University of Wyoming, on various federal privacy laws, such as the Electronic Communications Privacy Act, Fair Credit Reporting Act, Family Educational Rights and Privacy Act, Freedom of Information Act, Health Insurance Portability and Accountability Act, Privacy Act of 1974 and Federal Trade Commission Act. Mr. Sprague explained how the federal government addresses privacy laws sector by sector and how this has created a patchwork of laws with significant gaps. Mr. Sprague also mentioned that some federal laws, like the Electronic Communication Privacy Act which allows law enforcement access to an individual's electronic communications stored for over 180 days warrantless, were outdated. Of note, in June 2014, the U.S. Supreme Court held that police officers cannot search a cell phone seized incidental to an arrest without a warrant. *Riley v. California*, 134 S. Ct. 2473 (2014).

5. Enforcement of privacy protections

As to the enforcement of privacy protections, the Task Force heard from Flint Waters, Director, ETS, that the state lacked an affirmative obligation to protect personal data outside of W.S. 40-12-501 *et seq.*, the security breach notification statutes, and W.S. 6-3-901, the identify theft statute. Mr. Waters did note, however, that ETS had the authority under W.S. 9-2-2906(d) to establish and enforce data security policies and standards for the state data infrastructure. Mr. Waters suggested amending W.S. 9-2-2906(d) to grant the ETS authority to establish and enforce privacy policies and standards. Mr. Waters stated that these privacy policies and standards would be the minimum security requirements adhered to by all agencies operating in the executive branch of state government.

6. Other issues considered useful in encouraging appropriate safeguards for the privacy of digitally stored information

The Task Force heard testimony and received model legislation from several presenters on issues related to privacy interests in personal online accounts. One issue dealt with an employer requesting or requiring an employee or prospective employee to disclose a username or password to access a personal internet account. Robert Sprague, Associate Professor, University of Wyoming, expressed concern with the varying definitions of personal internet accounts and how many definitions failed to consider that internet accounts frequently serve both a personal and professional purpose. Mr. Sprague also recommended including provisions prohibiting waiver of rights and providing for a private right of action and escalating fines for repeated offenses.

A second issue dealt with access to a decedents' online communications. Carl Szabo, Policy Counsel, NetChoice, discussed the Model Fiduciary Access to Digital Assets Act which allows an electronic communication service or remote computing service to provide a personal representative access to or copies of the contents of the electronic communications of a deceased person upon receipt of specified documents. The Task Force was concerned with the permissive language of the model act and its deference to a company's privacy terms of service. The Task Force was persuaded that an individual's instructions specifying who has authority to access, transfer or terminate the individual's electronic communications after death should control.

A more in depth look at the topics covered by the Task Force can be found in the minutes of the Task Force available on the LSO website.

Recommendations

Proposed legislation

1. **15LSO-0066 F1.1 – Right of privacy-constitutional amendment.**

This bill proposes to amend the Wyoming Constitution to specify that the right to individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest.

2. **15LSO-0067 F1.1 – State protection of data privacy.**

This bill amends W.S. 9-2-2906(d) to require ETS to establish and enforce data privacy policies and standards for the state data infrastructure. This bill specifies that these data privacy policies and standards shall be the minimum privacy requirements adhered to by all state agencies.

3. **15LSO-0073 F1.1 – Employee online privacy.**

This bill prohibits an employer from requesting or requiring access to a personal internet account of an employee or prospective employee. This bill prohibits an employer from taking adverse action against an employee or prospective employee for failing to disclose information to access a personal internet account. This bill provides exceptions for (1) internet accounts or services provided by the employer, set up by the employee at the employer's request or used primarily for an employer's business purposes; (2) employer work-related investigations; (3) the enhancement of communications with an employee or prospective employee; and (4) information in the public domain. This bill also prohibits the waiver of rights and provides for civil penalties and a civil cause of action.

4. **15LSO-0074 F1.1 – Decedents' electronic communications.**

This bill grants personal representatives the authority to access, transfer or terminate a decedent's electronic communications unless such authority is contrary to the express provisions of a will, trust instrument, power of attorney or court order. This bill prohibits a cause of action against an electronic communication service or remote computing service for providing to the personal representative authority to access, transfer or terminate the decedent's electronic communications.

5. **15LSO-0075 F1.1 – Personal identifying information-definitions.**

This bill amends the definitions of personal identifying information in the identify theft statute and security breach notification statute to include, among other things, a username or email address, in combination with a password or security question and answer that would permit access to an online account; shared secrets, security tokens or knowledge based authentication; medical information; health insurance information; unique biometric data; and individual taxpayer identification number.

6. **15LSO-0133 F1.1 – Security breach notification.**

This bill requires an individual or entity to notify consumers affected by breaches of personal identifying information of the following: a general description of the breach and the type of personal identifying information that were or are reasonably believed to have been the subject of the breach; the approximate date of the breach; the actions taken to protect the system containing the personal identifying information from further breaches; advice to the consumer to review account statements and monitor credit reports; whether notification was delayed as a result of law enforcement investigation; and notice of the right to identity theft prevention and mitigation services. This bill provides for damages and requires an individual or commercial entity to provide identity theft prevention and mitigation services to affected Wyoming residents whose information was or may have been breached.

Staffing and support

The Task Force recommends that LSO staff and support the Task Force for the subsequent phases of the study.

Sincerely,

Senator Chris Rothfuss, Cochairman

Representative Mary Throne, Cochairman

Cc: Management Council