Legal Concepts Meet Technology: A 50 State Survey of Privacy Laws

Miriam B. Russom
University of Illinois at Chicago, Computer Science Department

Robert H. Sloan
University of Illinois at Chicago, Computer Science Department

Richard Warner
Chicago–Kent College of Law
We have lost a significant degree of control over how others use our personal information.

- What legal concepts of privacy have been developed in response to the changing technology?

- Are these responses adequate?
Outline

- Informational Privacy: Three Questions
- Methodology
- State Privacy and Security Laws
- Personally Identifying Information

Findings:
- PII
- Security Laws
- Privacy Laws

Conclusions
Informational Privacy Definition

“[T]he claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.”

Westin, 1967
Three key questions

➢ To what extent should we be able to control our information?

➢ What types of information should we protect?

➢ How should we protect it?
Methodology

- Detailed survey and analysis of current US state privacy laws
  - rich field of privacy regulations in which commonalities and differences reveal an underlying conception of informational privacy
- Surveyed statutes chosen for their relevance to contemporary informational privacy
  - Not an exhaustive compilation
  - Statutes mostly found in Trade and Commerce Codes, Business Codes, Customer Record laws, and Internet Privacy Codes.
# State Privacy and Security Laws

<table>
<thead>
<tr>
<th>Type of law</th>
<th>#</th>
<th>States</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Security</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Security measures requirement law</td>
<td>11</td>
<td>AK, CA, MD, MA, MN, NV, NC, OR, RI, TX, UT</td>
</tr>
<tr>
<td>Data Disposal/ Destruction law</td>
<td>30</td>
<td>AL, AZ, AK, CA, CO, CT, GA, HI, IL, IN, KS, KY, MD, MA, MI, MO, MT, NV, NJ, NY, NC, OR, RI, SC, TN, TX, UT, VT, WA, WI</td>
</tr>
<tr>
<td>Spyware law</td>
<td>16</td>
<td>AL, AZ, AK, CA, GA, IN, IA, LA, NV, NH, PA, RI, TX, UT, VA, WA</td>
</tr>
<tr>
<td><strong>Data Privacy</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Breach Notification law</td>
<td>46 (+ DC)</td>
<td>AL, AZ, AK, CA, CO, CT, DE, DC, FL, GA, HI, ID, IL, IN, IA, KS, LA, ME, MD, MA, MI, MN, MS, MO, MT, NE, NV, NH, NJ, NY, NC, ND, OH, OK, OR, PA, RI, SC, TN, TX, UT, VT, VA, WA, WV, WI, WY</td>
</tr>
<tr>
<td>Online Privacy law</td>
<td>2</td>
<td>MN, NV</td>
</tr>
<tr>
<td>Data Sharing law</td>
<td>2</td>
<td>CA, UT</td>
</tr>
<tr>
<td>Privacy Policy on Web sites requirement law</td>
<td>4</td>
<td>CA, CT, PA, NB</td>
</tr>
<tr>
<td>Health Information Privacy</td>
<td>15</td>
<td>CA, ME, MI, MS, NE, NJ, NM, ND, OR, TN, TX, VA, WA, WI, WY</td>
</tr>
<tr>
<td>Genetic Information Privacy</td>
<td>37</td>
<td>AL, AK, CA, CO, DE, FL, GA, HI, ID, IL, IA, LA, MD, MA, MI, MN, MO, NE, NV, NH, NJ, NM, NY, OR, RI, SC, SD, TN, TX, UT, VT, VA, WA, WV, WI, WY</td>
</tr>
<tr>
<td>Insurance Information Privacy</td>
<td>16</td>
<td>CA, CT, ME, MA, MI, MN, MT, NE, NM, ND, OH, OK, OR, PA, VA, WA</td>
</tr>
<tr>
<td>Financial Information Privacy</td>
<td>19</td>
<td>AL, CA, CT, FL, IL, ME, MD, MN, MS, MO, NH, NC, ND, OK, OR, SC, TN, UT, WA</td>
</tr>
</tbody>
</table>
# Personally Identifying Information

<table>
<thead>
<tr>
<th></th>
<th>Data Disposal</th>
<th>Breach Notification</th>
<th>Security Measures</th>
<th>Spyware</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>30 states</td>
<td>46 + DC</td>
<td>11 states</td>
<td>16 states</td>
</tr>
<tr>
<td><strong>Driver license #</strong></td>
<td>AL, AZ, AK, CA, CO, CT, GA, HI, IL, IN, KS, KY, MD, MA, MI, MT, NV, NJ, NY, NC, OR, RI, SC, TN, TX, UT, VT, WA</td>
<td>AL, AZ, AK, CA, CO, CT, DE, DC, FL, GA, HI, ID, IL, IN, IA, KS, LA, ME, MD, MA, MI, MN, MS, MO, MT, NE, NV, NH, NJ, NY, NC, ND, OH, OK, OR, PA, RI, SC, TN, TX, UT, VT, VA, WA, WV, WI, WY</td>
<td>AK, CA, MA, MD, NV, NC, OR, RI, TX, UT</td>
<td>AZ, CA, IN, NH, PA, RI, UT, VA, WA</td>
</tr>
<tr>
<td><strong>state identification #</strong></td>
<td>All above excluding AL</td>
<td>All above</td>
<td>All above</td>
<td>All above including AK, GA, IA, LA, TX</td>
</tr>
<tr>
<td><strong>Social Security #</strong></td>
<td>All above including WI</td>
<td>All above excluding CO</td>
<td>All above</td>
<td>Same as immediately above</td>
</tr>
<tr>
<td><strong>Financial Account/ Credit/ Debit Card #</strong></td>
<td>All above including WI</td>
<td>All above excluding CO</td>
<td>All above</td>
<td>Same as immediately above</td>
</tr>
<tr>
<td>PII</td>
<td>Data Disposal</td>
<td>Breach Notification</td>
<td>Security Measures</td>
<td>Spyware</td>
</tr>
<tr>
<td>-----</td>
<td>---------------</td>
<td>---------------------</td>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Address</td>
<td>CA, KY</td>
<td>DC, MN</td>
<td>MN</td>
<td>AZ, AK, CA, GA, IN, IA, LA, NH, PA, RI, TX, UT, VA, WA</td>
</tr>
<tr>
<td>Biometric data</td>
<td>CO, MA, NC, TN, TX</td>
<td>IA, NE, NC, WI</td>
<td>NC</td>
<td>IN, UT</td>
</tr>
<tr>
<td>DNA</td>
<td></td>
<td>WI</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fingerprints</td>
<td>KY, NC, TX</td>
<td>NC, WI</td>
<td>NC</td>
<td>IN</td>
</tr>
<tr>
<td>Voice print</td>
<td>TX</td>
<td>WI</td>
<td></td>
<td>IN</td>
</tr>
<tr>
<td>Digital signature</td>
<td>NC</td>
<td>NC, ND</td>
<td>NC</td>
<td>UT</td>
</tr>
<tr>
<td>Employment inf.</td>
<td>AL, CA, CO</td>
<td>ND</td>
<td></td>
<td>IN, UT</td>
</tr>
<tr>
<td>E-mail address</td>
<td>KY, NC</td>
<td>MN, NC</td>
<td>MN, NC</td>
<td>AZ, IN, NH, RI, TX, WA</td>
</tr>
<tr>
<td>Health insurance inf.</td>
<td>AL, CA, CT, RI, TN</td>
<td>CA, MO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medical inf.</td>
<td>AL, AK, CA, KY, RI, WA, WI</td>
<td>AK, CA, MO, TX</td>
<td>AK, CA, TX</td>
<td></td>
</tr>
<tr>
<td>Mother's maiden name</td>
<td>NY, TX</td>
<td>ND</td>
<td></td>
<td>IN</td>
</tr>
<tr>
<td>Passwords</td>
<td>CO, NC, TN</td>
<td>GA, IA, MO, NE, NC</td>
<td>NC</td>
<td>NH, UT</td>
</tr>
<tr>
<td>Payment / Overdraft history</td>
<td></td>
<td></td>
<td></td>
<td>AZ, AK, CA, GA, IN, LA, PA, RI, TX, WA</td>
</tr>
<tr>
<td>Physical description</td>
<td>CA, RI</td>
<td>WI</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phone number</td>
<td>CA, KY</td>
<td>DC, MN</td>
<td>MN</td>
<td>IN, NH, UT</td>
</tr>
<tr>
<td>Record of purchases</td>
<td></td>
<td></td>
<td></td>
<td>AK, CA, GA, LA, PA</td>
</tr>
<tr>
<td>Routing code</td>
<td>TX</td>
<td>IA, MO, NE</td>
<td></td>
<td>IN</td>
</tr>
<tr>
<td>Web history</td>
<td></td>
<td>MN</td>
<td>MN</td>
<td>AK, CA, GA, LA, PA</td>
</tr>
</tbody>
</table>
Findings: State Laws

- CA has almost every statutes followed by UT

- Almost every state has Breach Notification Law (except for AL, KY, NM, SD)
  - KY has only Data Disposal Law (all states that have DD and DS have also BN)

- Only Breach Notification: #10
  - DE, DC, FL, ME, MS, ND, OH, OK, WV, WY

- States with all 3 type of security laws: #5
  - AK, CA, NV, TX, UT

- Spyware but not Data Security: #8
  - AZ, IN, IA, LA, NH, PA, VA, WA

- Very few states have statutes on limitation of use of PII
Findings: PII

- Almost every state agrees on:
  - Social Security number; Driver License number; Financial accounts;

- Otherwise no general agreement on what information should be legally protected.
  - Significant state to state variations as well as variations within a state among the different types of statutes.

- Some examples:
  - TN specifies Biometric Data, Health Insurance Information and Password only in Data Disposal. Likewise, TX specifies Biometric data, Mother’s maiden name, routing code only in Data Disposal.
  - IN and UT are the only ones having Biometric data, employment information in Spyware. UT only includes Digital signature and IN only includes routing code and mother’s maiden name. However neither UT nor IN include Record of purchases and Web history while other states do.
  - MN and NC define consistently PII over all of the surveyed statutes.
Concern: Non-PII = PII?

Recent advances in de-anonymization ensure that, in very many cases, non-PII may in fact identify individuals.

- MIT graduate student, Latanya, identified the anonymized medical records of the Governor of Massachusetts
- Netflix Prize: Narayanan and Shmatikov identified the anonymous Netflix records of an individual by cross linking with internet movie database based on dates and titles of movie reviews
Losses from unauthorized access to online information run in the billions per year.

- Average cost of a data breach was $214 per compromised record and $7.2 million per data breach [2010 study by Ponemon Institute]

**But:** Only 11 States require businesses to adopt reasonable security measures to protect the collected PII.

**Reasonableness requirements**

- Only 2 states, MA and NV, impose specific measures of reasonableness and encryption requirements of both data at rest and in transit.

- More specific security measures requirements?
Security: Data Disposal Laws

**Reasonableness requirements:** 11 out of 30 states require the use of reasonable standards of disposal of records that contain PII when the data is no longer needed.

**More than reasonableness: (almost no guidance at all)**

- Shredding
- Erasing
- Modifying the PII to make it unreadable by any means
Security: Anti-Spyware Laws

16 States have enacted Anti-Spyware laws that make it illegal to install software *without consent* on someone else's computer in order to collect PII.

But:

- Consumers do not read standard form contracts.
- So what are they doing when they use websites or buy products?
- Consumers indicate merely their willingness to proceed with the transaction--not necessarily their free and informed consent.
Privacy: Breach Notification Laws

Forty-six states and DC have enacted security breach notification laws that require organizations that own or license personal information to notify individuals when unauthorized access to PII has occurred.

**Rationale:** consumer can take protective steps to prevent identity theft, financial fraud, or other undesirable consequences.

- Low individual expected losses vs. aggregate losses that run in the billions.
- Empowering consumers to defend themselves may not be a viable response to the problem of aggregate loss.
Privacy: Data Sharing Laws

There are no laws that regulate private business data sharing generally. The states regulate data sharing only through subject-specific statutes.

- California requires a business to disclose, upon consumer request, the type of PII it shared and the third parties with whom it shared the information.
- Utah requires commercial entities with the intention to sell personal information to notify the customer.
- Two states, Minnesota and Nevada, require consent from the subject of the information before an ISP may disclose PII.
Privacy: Access and Correction Requirements

None of the laws surveyed so far give an individual the right to access and correct records.

- Data sharing laws discussed above provide some access but do not allow correction

Problems with access and correction

- Automated checking's and correction problematic.
- Very large number of requests could impose serious costs.
- Access alone provides little control unless the consumer has power to correct errors.
Conclusions

- **How much control should we have over our information?**
  - The surveyed laws fail to address this issue

- **What types of information should we protect?**
  - Lack of consensus on what to protect under the PII rubric
  - Difficulties to delimit PII

- **How should we protect private information?**
  - Data security laws rely on reasonableness standards
  - In-practice consent is taken as sufficient for authorization
  - Little legal constraints on data sharing
  - Practical and technical problems with access and correction
  - Large aggregate costs vs low individual expected costs
Thank you!