CA’s Privacy Legal Framework

• Reasonable Security
  – Minimum standard of “reasonable security”

• Consumer Notice
  – California Online Privacy Protection Act
Civil Code § 1798.81.5

A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.
2016 Data Breach Report

4 years of breaches affecting >500 CA residents (2012-2015)
- 657 breaches
- 49+ million records of CA residents breached
Greatest Threat:

- Malware & hacking, both in the number of breaches and the number of records breached.
  - 54% total breaches,
  - 90% of records breached = 44.6 million records.

Industry Hardest Hit:

- Retail, with 25% of breaches, 42% records
  - Type of Data: Payment Cards
• The 20 controls in the Center for Internet Security’s Critical Security Controls define a minimum level of information security that all organizations that collect or maintain personal information should meet. **The failure to implement all the Controls that apply to an organization’s environment constitutes a lack of reasonable security.**
# CIS Critical Security Controls

<table>
<thead>
<tr>
<th>CSC 1</th>
<th>Inventory of Authorized and Unauthorized Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSC 2</td>
<td>Inventory of Authorized and Unauthorized Software</td>
</tr>
<tr>
<td>CSC 3</td>
<td>Secure configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers</td>
</tr>
<tr>
<td>CSC 4</td>
<td>Continuous Vulnerability Assessment and Remediation</td>
</tr>
<tr>
<td>CSC 5</td>
<td>Controlled Use of Administrative Privileges</td>
</tr>
<tr>
<td>CSC 6</td>
<td>Maintenance, Monitoring, and Analysis of Audit Logs</td>
</tr>
<tr>
<td>CSC 7</td>
<td>Email and Web Browser Protection</td>
</tr>
<tr>
<td>CSC 8</td>
<td>Malware Defenses</td>
</tr>
<tr>
<td>CSC 9</td>
<td>Limitation and Control of Network Ports, protocols, and Services</td>
</tr>
<tr>
<td>CSC 10</td>
<td>Data Recovery Capability</td>
</tr>
</tbody>
</table>
## CIS Critical Security Controls

<table>
<thead>
<tr>
<th>CSC 11</th>
<th>Secure Configurations for Network Devices (Firewalls, Routers, Switches)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSC 12</td>
<td>Boundary Defense</td>
</tr>
<tr>
<td>CSC 13</td>
<td>Data Protection</td>
</tr>
<tr>
<td>CSC 14</td>
<td>Controlled Access Based on the Need to Know</td>
</tr>
<tr>
<td>CSC 15</td>
<td>Wireless Access Control</td>
</tr>
<tr>
<td>CSC 16</td>
<td>Account Monitoring and Control</td>
</tr>
<tr>
<td>CSC 17</td>
<td>Security Skills Assessment and Appropriate Training to Fill Gaps</td>
</tr>
<tr>
<td>CSC 18</td>
<td>Application Software Security</td>
</tr>
<tr>
<td>CSC 19</td>
<td>Incident Response and Management</td>
</tr>
<tr>
<td>CSC 20</td>
<td>Penetration Tests and Red Team Exercises</td>
</tr>
</tbody>
</table>
Next Challenge for Security: IoT

Attorney General Kamala D. Harris Urges Consumers to Protect their Devices from Potential “Botnet Attacks”

Monday, October 31, 2016
Contact: (415) 703-5837, agpressoffice@doj.ca.gov

LOS ANGELES – Attorney General Kamala D. Harris is advising Californians to protect their electronic devices from potential hacks and urges Internet of Things (IoT) manufacturers and developers to take immediate steps to help secure home electronic devices against capture by a potential “botnet attack” from a cyber criminal.

The IoT includes connected devices and smart devices, including everyday objects such as webcams, routers, DVRs, lighting, heating, and refrigerators. A botnet is a network of infected computers, where the network is used by the malware to expand. A botnet attack occurs without the computer owners’ knowledge, and is typically used to send spam emails, transmit viruses, and engage in other acts of cybercrime.

As recent botnet attacks have shown, a greater emphasis on the security of connected devices, with a focus on security-by-design in product development, is urgent and essential. Much is at stake as IoT continues its rapid expansion to an estimated 38 billion connected devices by 2020. Improving the security of these devices will make
Connected Toothbrush
Internet of Things Security Companion to the CIS Critical Security Controls (Version 6)
An operator of a commercial Web site or online service that collects PII through the Internet about individual consumers residing in California who use or visit its commercial Web site or online service shall *conspicuously post* its privacy policy on its Web site.
CalOPPA Complaint Tool

State of California
Department of Justice

Xavier Becerra ~ Attorney General

CALOPPA COMPLAINT FORM

Please use this form to report potential violations of the California Online Privacy Protection Act (Bus. & Prof. Code §§ 22575-22579) by websites and online services (such as mobile apps). A website, app, or other online service may violate this law if:

- It lacks a privacy policy
- Its privacy policy is hard to find
- Its privacy policy does not contain all the information required by law
- It does not follow its own privacy policy, or
- It does not notify users of significant changes to its privacy policy

SECTION 1:
THE COMPANY YOU ARE REPORTING

Company Name: *

Company Website:
http://

App Name (if applicable):

Please identify the nature of the alleged noncompliance by checking one or more of the boxes below. *

- [ ] Privacy Policy Missing or Inapplicable

Privacy and Online Security

Privacy Home
Consumer Privacy Resources
Identity Theft
Protecting Children Online
Business Privacy Resources
Privacy Enforcement, Laws, and Legislation
Privacy Reports
Special Protection
Privacy and Piracy Fund
Notice to Consumers

We are always looking for ways to improve our customers’ shopping experience. Nordstrom is using Euclid to gather publicly-broadcasted information your Smartphone or other Wi-Fi enabled device sends out when it’s attempting to connect to a Wi-Fi network in and around this store. Euclid provides Nordstrom with anonymous, aggregate reports that give us a better sense of customer foot traffic. We do not gather such things as your name, email address, phone number, your device’s browsing activity or text, email or voice messages.

To not participate, turn off your device’s Wi-Fi function or power off your device.

To opt-out or learn more about Euclid, visit http://euclidanalytics.com/privacy.
You can also visit http://shop.nordstrom.com/c/nordstrom-privacy.
Privacy Best Practice Recommendations For Commercial Facial Recognition Use

These “Privacy Best Practice Recommendations for Commercial Facial Recognition Use” serve as general guidelines for covered entities. The fundamental principles underlying the recommendations are based on the Fair Information Practice Principles (FIPPs). It is left to implementers and operators to determine the most appropriate way to implement each of these privacy guidelines.

Given the numerous existing uses in widely different applications (such as authentication, social media, and physical access control), as well as potential uses, specific/detailed practices are not feasible or practical across this wide spectrum. These best practices are intended to provide a flexible and evolving approach to the use of facial recognition technology, designed to keep pace with the dynamic marketplace surrounding these technologies.

This document is intended to provide a general roadmap to enable entities using facial recognition technologies by recognizing differing objectives, risks, and individual expectations associated with various applications of these technologies.

These principles do not apply to the use of a facial recognition for the purpose of aggregate or non-identifying analysis. For example, when facial recognition technology is used only to count the number of unique visitors to a retail establishment or to measure the genders or approximate ages of people who view a store display (for marketing research purposes), those practices are outside the scope of these principles.

These best practices do not apply to security applications, law enforcement, national security, intelligence or military uses, all of which are beyond the scope of this document.

Definitions

Covered Entity – Any person, including corporate affiliates, that collects, stores, or processes facial template data. Covered entities do not include governments, law enforcement agencies, national security agencies, or intelligence agencies.

Unaffiliated Third Party – Any person other than (1) a user of a covered entity’s products or services; (2) a covered entity’s employees; (3) an entity under common control or ownership with a covered entity; or (4) a vendor or supplier to a covered entity when such vendor or supplier is used to provide a product or service related to facial template data.

Facial Template Data – A unique facial attribute or measurement generated by automatic measurements of an individual’s facial characteristics, which are used by a covered entity to

1 FIPPs are a widely accepted framework of defining principles to be used in the evaluation and consideration of systems, processes, or programs that affect individual privacy. These principles are at the core of the Privacy Act of 1974 and are mirrored in the laws of many U.S. states, as well as in those of many foreign nations and international organizations.
Resources from CA AG

• Business Privacy Resources
  – www.oag.ca.gov/privacy/business-privacy

• California Data Breach Reports
  – www.oag.ca.gov/privacy/privacy-reports

• Data Breach Reporting
  – www.oag.ca.gov/ecrime/databreach/reporting

• Privacy Enforcement Actions, Laws, & Legislation
  – www.oag.ca.gov/privacy/privacy-enforcement-laws-legislation
Civil Code § 1798.82

• “breach of the security of the system”
• “most expedient time possible and without unreasonable delay”
• “notification shall be written in plain language” (new format reqs.)
• “provide appropriate identity theft prevention and mitigation services” (SSN or DL)
• >500 CA, provide sample copy of notice to AG