Privacy & Data Security:
Legal Risks for Software Developers

Detroit Dev Day
November 14, 2015

Tatiana Melnik
Melnik Legal PLLC
tatiana@melniklegal.com
734-358-4201
Tampa, FL

Outline

I. Regulating Privacy and Data Security

II. Is Someone Regulating Software?

A. Federal Enforcement
B. State Enforcement
C. Private Enforcement
D. Costs of a Data Breach
E. Personal Liability

Outline

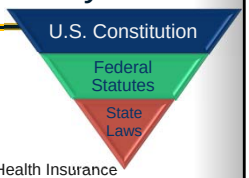
I. Regulating Privacy and Data Security

II. Is Someone Regulating Software?

A. Federal Enforcement
B. State Enforcement
C. Private Enforcement
D. Costs of a Data Breach
E. Personal Liability

The Foundation of Privacy

- **Federal Laws**
  - US Constitution
  - Statutes
    - Federal Trade Commission Act (1914) - Section 5
    - Electronic Communications Privacy Act (1986)
    - Computer Security Act (1987)
    - Gramm-Leach-Bliley Act (1999)
    - Sarbanes-Oxley Act (2002)
    - Health Insurance Portability and Accountability Act (1996) and the more recent Health Information Technology for Economic and Clinical Health Act (2009)
    - ***Many more…***
  - Regulations



U.S. Constitution

- **Supreme Court Cases**
  - *Griswold v. Connecticut* – **Where is privacy?**
    - Court struck down Connecticut law prohibiting the sale and use of birth control because it intruded on the right of marital privacy
    - Right of privacy to found in "emanations" and "penumbras" (shadows) of other constitutional protections
  - *Roe v. Wade* – **Balancing act**
    - Recognized a woman's decision to choose, but balanced against the states' interests in protecting women's health and human life
  - *Whalen v. Roe* – **Privacy vs. the public interest**
    - Court upheld a New York provision regarding reporting requirements for Schedule II drug prescriptions as being within the states' police power to deal with crime

U.S. Constitution

- **Context Matters**
  - **"The Constitution does not explicitly mention any right of privacy"** - *Roe v. Wade*
  - "**Zones of privacy**" - *Griswold v. Connecticut*
    - First Amendment: Right of association
    - Third Amendment: Right not to have to quarter soldiers
    - Fourth Amendment: Right against unreasonable search and seizure (feel "*secure in their persons, houses, papers and effects*")
    - Fifth Amendment: Right against self-incrimination
    - Ninth Amendment: Preservation of unenumerated rights (rights "*retained by the people*")

This slide presentation is informational only. It does not constitute legal or professional advice. You are encouraged to consult with an attorney if you have specific questions relating to any of the topics covered in this presentation, and Melnik Legal PLLC would be pleased to assist you in these matters.

U.S. Constitution

- **Context Matters**
  - Justice Potter Stewart's famous quote, holding that the Constitution protected all obscenity except "hard-core pornography."

U.S. Constitution

- **Context Matters**
  - Justice Potter Stewart's famous quote,

Stewart wrote:

"I shall not today attempt further to define the kinds of material I understand to be embraced within that shorthand description; and perhaps I could never succeed in intelligibly doing so. ***But I know it when I see it***, and the motion picture involved in this case is not that."

Federal Legislation

- **Context Still Matters**
  - **Targeted Information**
    - Financial (GLBA)
    - Medical (HIPAA)
  - **Targeted Constituency**
    - Consumers (FTC Section 5)
    - Children (COPPA)
  - **Segregation of Super Private Information**
    - STDs
    - Mental health
  - **Obligations for using particular information**
    - Substance abuse

State Laws

- Social Security Numbers
- Drivers licenses
- Protection of health care information
- Recordkeeping and data destruction
- Breach disclosure

State Laws

What is PII?

What state are you in?

- ☐ Social Security Number
- ☐ Credit / Debit Card Number (with a pin no.)
- ☐ Medical history or treatment
- ☐ Health insurance policy number
- ☐ Username or e-mail address plus password
- ☐ "Any other identifier that permits the physical or online contacting of a specific individual"

Industry Standards

- EHNAC (Electronic Healthcare Network Accreditation Commission)
  - an independent, federally recognized, standards development organization
- PCI DSS
- NIST
  - sets standards for U.S. federal agencies, which often become the de-facto standards throughout industry because of the scope of government contracting

This slide presentation is informational only. It does not constitute legal or professional advice. You are encouraged to consult with an attorney if you have specific questions relating to any of the topics covered in this presentation, and Melnik Legal PLLC would be pleased to assist you in these matters.

International Laws

- **E.U. Privacy Directive 95/46/EC**
  - Addresses the collection, use, processing, and movement of personal data
- **E.U. Internet Privacy Law of 2002** (Directive 2002/58/EC)
  - Protects data in electronic transactions
- Individuals countries have their own laws

What do the Laws Cover?

- What information can be collected
- How it must be stored and secured
- Under what circumstances it can be shared
- Responding to data breaches and data losses
- Penalties for data breaches and data losses
- Exemptions for federally regulated industries

Outline

I. Regulating Privacy and Data Security

II. **Is Someone Regulating Software?**

A. Federal Enforcement
B. State Enforcement
C. Private Enforcement
D. Costs of a Data Breach
E. Personal Liability

Enforcement Landscape

- Who is Enforcing Privacy and Security?

Federal Trade Commission
- Credit Unions
- Banks
- Credit Card Companies
- Insurance Companies

HHS Office of Civil Rights

Consumers

State's Attorneys' General
- SEC
- **FCC (Nov. 5, 2015)
- Insurance Regulators
- FFIEC
- NYDFS
- OIG Audits

Federal Trade Commission

Federal Trade Commission

- Works for **consumers** to prevent fraudulent, deceptive, and unfair business practices
- Section 5 – "**unfair or deceptive acts or practices** in or affecting commerce ...are... declared unlawful."
- Has authority to pursue **any company**
- Has pursued companies across a number of industries

Federal Trade Commission

- Practices the FTC finds problematic
  - Improper use of data
  - Retroactive changes
  - Deceitful data collection
  - Unfair data security practices

For a more detailed analysis, *see* Daniel J. Solove & Woodrow Hartzog, The FTC and the New Common Law of Privacy, Columbia Law Review (2014)

This slide presentation is informational only. It does not constitute legal or professional advice. You are encouraged to consult with an attorney if you have specific questions relating to any of the topics covered in this presentation, and Melnik Legal PLLC would be pleased to assist you in these matters.

Federal Trade Commission

- **In the Matter of HTC America, Inc.**
  - July 2013
  - Phone and software manufacturer, using Android and Windows operating systems
  - Allegation:
    - company ***failed to take reasonable steps to secure the software it developed for its smartphones and tablet computers***, introducing security flaws that placed sensitive information about millions of consumers at risk

Federal Trade Commission

- **What did the FTC allege HTC did wrong?**
  - respondent engaged in a number of practices that, ***taken together***, **failed to employ reasonable and appropriate security in the design and customization of the software** on its mobile devices
  - **Assess Security** - failed to implement an adequate program to assess the security of products it shipped to consumers
  - **Provide Guidance and Training** - failed to implement adequate privacy and security guidance or training for its engineering staff

Federal Trade Commission

- **Testing and auditing** - failed to conduct assessments, audits, reviews, or tests to identify potential security vulnerabilities in its mobile devices
- **Failed to follow standards** - failed to follow well-known and commonly-accepted secure programming practices, including secure practices that were expressly described in the operating system's guides for manufacturers and developers, which would have ensured that applications only had access to users' information with their consent

Federal Trade Commission

- **No communication** - failed to implement a process for ***receiving and addressing security vulnerability reports*** from third-party researchers, academics or other members of the public, thereby delaying its opportunity to correct discovered vulnerabilities or respond to reported incidents
- **HTC introduced numerous security vulnerabilities in the process of customizing its mobile devices**

Federal Trade Commission

- Introduced numerous **permission re-delegation vulnerabilities** through its custom, pre-installed applications
  - Because no check, third party apps could enable the device's microphone; access the user's GPS-based, cell-based, and WiFi-based location information; and send text messages -- **all without requesting the user's permission**
  - ***could have prevented this by including simple, well-documented software code – "permission check" code***

Federal Trade Commission

- Failed to use **readily-available and documented *secure* communications mechanisms** in implementing logging applications on its devices, placing sensitive information at risk
  - Instead of using one of these well-known, secure alternatives [(*e.g.*, Android inter-process, secure UNIX sockets)], ***HTC implemented communication mechanisms*** (*e.g.*, INET sockets) ***that could not be restricted in a similar manner***
  - Failed to implement other, ***additional security measures (e.g., data encryption***) that could have secured these communications mechanisms

This slide presentation is informational only. It does not constitute legal or professional advice. You are encouraged to consult with an attorney if you have specific questions relating to any of the topics covered in this presentation, and Melnik Legal PLLC would be pleased to assist you in these matters.

Federal Trade Commission

- HTC failed to **deactivate the debug code** before its devices shipped for sale to consumers
  - HTC ***could have detected its failure to deactivate the debug code in its CIQ Interface had it had*** adequate processes and tools in place for reviewing and testing the security of its software code

Federal Trade Commission

- HTC settled with the FTC – agreed to:
  - **Establish, implement, and maintain, a comprehensive security program** that is reasonably designed to
    - (1) address security risks related to the development and management of new and existing covered devices, and
    - (2) protect the security, confidentiality, and integrity of covered information, whether collected by respondent or input into, stored on, captured with, accessed or transmitted through a covered device.
      - Such program, the content and implementation of which must be fully documented in writing, shall **contain administrative, technical, and physical safeguards** appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the covered device functionality or covered information, **including**:

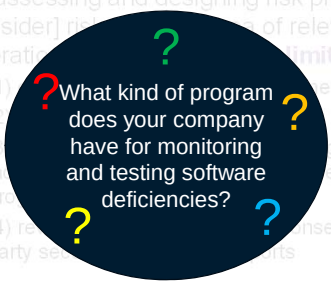
Federal Trade Commission

- designation of an employee or employees to coordinate and be **accountable** for the security program
- **identification of** material internal and external **risks** to the security of covered devices that could result in unauthorized access to or use of covered device functionality, **and assessment of** the sufficiency of any **safeguards** in place to control these risks

Federal Trade Commission

- [in assessing and designing risk program, consider] risks in each area of relevant operation, **including, but not limited to**:
  - (1) employee training and management;
  - (2) product design, development and research;
  - (3) secure software design and testing, including secure engineering and defensive programming; and
  - (4) review, assessment, and response to third-party security vulnerability reports

Federal Trade Commission



Federal Trade Commission

- HTC has a **20 year compliance period**
  - Every two years, must get a third party audit that
    - Evaluates its "administrative, technical, and physical safeguards"
    - Certifies that its "security program is operating with sufficient effectiveness to provide reasonable assurance that the security of covered device functionality and the security, confidentiality, and integrity of covered information is protected and has so operated throughout the reporting period"

This slide presentation is informational only. It does not constitute legal or professional advice. You are encouraged to consult with an attorney if you have specific questions relating to any of the topics covered in this presentation, and Melnik Legal PLLC would be pleased to assist you in these matters.

Federal Trade Commission

- GMR Transcription Services, Inc. & the Two Principal Owners
  - Providers of medical transcription services
  - Liability based on action of contractor
  - Company = 20 years compliance

Federal Trade Commission

- GMR Transcription Services, Inc. & the

IT IS FURTHER ORDERED that respondents **Prasad and Srivastava [(the individual owners)]**, for a period of **TEN (10) YEARS** after the date of issuance of the order, shall notify the Commission of the following:

(a) Any changes to . . . **residence, mailing addresses and/or telephone numbers**, within ten (10) days of the date of such change;

(b) Any changes in . . . **employment status (including self-employment), and any changes in ownership in any business entity**, within ten (10) days of the date of such change. Such notice shall include: [lots of stuff]; and

(c) Any changes in . . . **name or use of any aliases or fictitious names**, including "doing business as" names.

HHS Office of Civil Rights

HHS Office of Civil Rights

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

- Enforces HIPAA
- HITECH Act (2009) expanded the scope of coverage to authorize enforcement authority over certain vendors (BAs)
  - By OCR
  - State AGs
- Mandatory penalties

HHS Office of Civil Rights

HHS Office of

- Enforces HIPAA
- HITECH Act (2009)

Violation - § 1176(a)(1)	Each violation	All such violations of an identical provision in a calendar year
Did Not Know	$100–$50,000	$1.5 M
Reasonable Cause	$1,000–$50,000	$1.5 M
Willful Neglect - Corrected	$10,000–$50,000	$1.5 M
Willful Neglect - Not Corrected	$50,000	$1.5 M

- Mandatory penalties

HHS Office of Civil Rights

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Covered Entities
healthcare providers, health plans, etc.

- Business Associate – IT Management Company
- Business Associate – EHR Vendor
- Business Associate – Mobile App Developer
- Business Associate – Integration Specialist

- Subcontractor – Data Destruction Vendor
- Subcontractor – Interface Developments
- Subcontractor – Data Center
- Subcontractor – Analytics Firm

HHS Office of Civil Rights

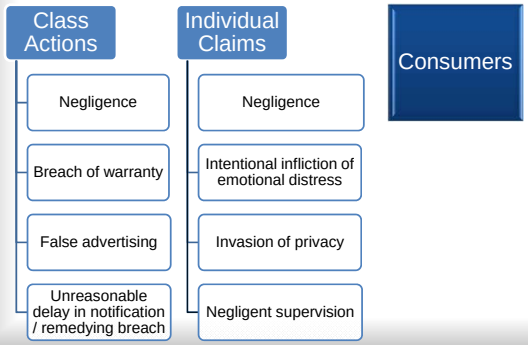
U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

- Enforcement by HHS Office of Civil Rights
  - To date ~25 organizations have paid out a total **$23M+** in settlements (with one fine)

- Cignet Health (**$4.3M**) (**fine**)
- UCLA Health System ($865,500)
- Blue Cross Blue Shield of TN ($1.5)
- **Alaska Dept. of Health & Human Services** ($1.7M)
- Massachusetts Eye and Ear Infirmary ($1.5M)
- Adult & Pediatric Dermatology ($150K)
- New York & Presbyterian Hospital (**$3M**) (**settlement**)
- Columbia University ($1.5M)
- Parkview Health System ($800K)
- Anchorage Community Mental Health Services ($150K) (unpatched and unsupported software → malware)
- Cornell Prescription Pharmacy ($125K)
- St. Elizabeth's Medical Center ($218K) (document sharing software)
- Cancer Care Group ($750K) (Aug. 31)

This slide presentation is informational only. It does not constitute legal or professional advice. You are encouraged to consult with an attorney if you have specific questions relating to any of the topics covered in this presentation, and Melnik Legal PLLC would be pleased to assist you in these matters.

Private Enforcement



Private Enforcement

Abigail E. Hinchy v. Walgreen Co. et al. (Indiana Superior Ct., 2013)

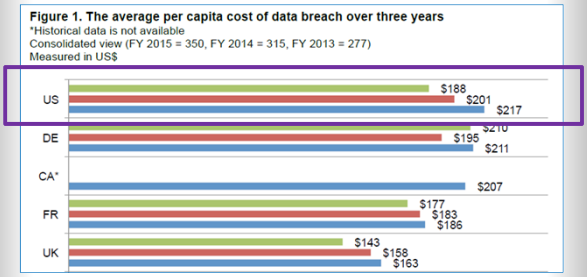
- Pharmacist improperly accessed medical records of one patient
- Patient reported the incident to Walgreen but Walgreen's **software did not log accesses**
- Once Walgreen learned of the employee, it did not disable the pharmacist's access
- Jury awarded $1.8 million, with $1.4M of that to be paid by Walgreens

Private Enforcement

- **Target as a case study**
  - Sued by at least 5 banks
  - Sued by each of the 4 major payment card networks
    - Settled with Visa to pay up to $67M
  - More than 100 lawsuits
    - Settled the consumer class action for $10M
  - Investigated by State Attorneys General, the FTC and the SEC
  - Through Aug. 1, 2015, the data breach has cost Target **$419 million** (with $150 million covered by insurance) (see Form 10-Q from 8/25/2015)

Costs of a Data Breach

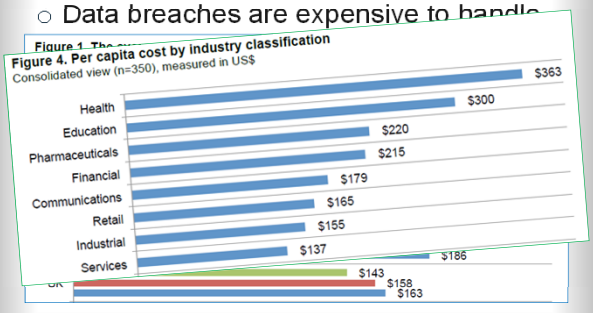
- Data breaches are expensive to handle



Source: Ponemon Institute, 2015 Cost of Data Breach Study: Global Analysis (May 2015)

Costs of a Data Breach

- Data breaches are expensive to handle



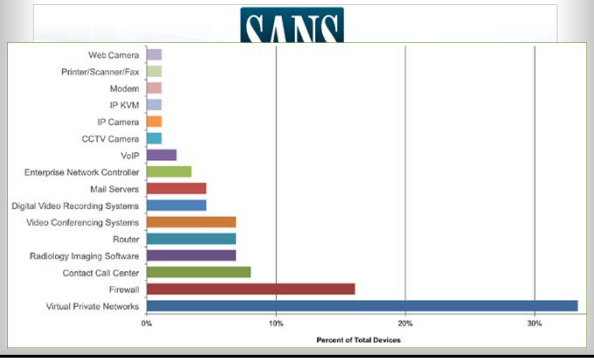
Source: Ponemon Institute, 2015 Cost of Data Breach Study: Global Analysis (May 2015)

Software Matters

- Processed and analyzed over 100 terabytes of traffic daily
  - 49,917 unique malicious events
  - 723 unique malicious source IP addresses
  - 375 U.S.-based compromised health care-related organizations

This slide presentation is informational only. It does not constitute legal or professional advice. You are encouraged to consult with an attorney if you have specific questions relating to any of the topics covered in this presentation, and Melnik Legal PLLC would be pleased to assist you in these matters.

Software Matters



Personal Liability

- Do software developers have any personal liability?
  - It depends….
    - What happened?
    - What was your role?
    - What is your role in the organization?
- Personal ethics and doing the right thing
  - Whistleblowers
    - *Qui tam*
    - Direct reporting (*see e.g.*, St. Elizabeth's Medical Center)

Three Final Thoughts…

- Co

Wh
sto
yo

Wh
soc
you

IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

In re: The Home Depot, Inc. Customer Data Breach Litigation	)	MDL No. 14-02583-TWT
This Document Relates to: All Financial Institution Cases	)	CONSOLIDATED CLASS ACTION COMPLAINT
	)	JURY TRIAL DEMANDED

FINANCIAL INSTITUTION PLAINTIFFS' CONSOLIDATED CLASS ACTION COMPLAINT

"If we rewind the tape, our security systems could have been better…Data security just wasn't high enough in our mission statement."

Frank Blake, Home Depot's recently retired Chief Executive Officer and Current Chairman of the Board

Disclaimer

This slide presentation is informational only and was prepared to provide a brief overview of enforcement efforts related to data privacy and security. It does not constitute legal or professional advice.

You are encouraged to consult with an attorney if you have specific questions relating to any of the topics covered in this presentation, and Melnik Legal PLLC would be pleased to assist you on these matters.

Any Questions?

Tatiana Melnik
Attorney, Melnik Legal PLLC
Based in Tampa, FL

734.358.4201
tatiana@melniklegal.com

This slide presentation is informational only. It does not constitute legal or professional advice. You are encouraged to consult with an attorney if you have specific questions relating to any of the topics covered in this presentation, and Melnik Legal PLLC would be pleased to assist you in these matters.