

2011 Thomas M. Cooley Law
Review's Annual Symposium: *Who's*
Mining Your Business?

**Fools' Gold: Privacy Protection &
Data Mining**

Jason M. Shinn

www.ebusinesscounsel.com

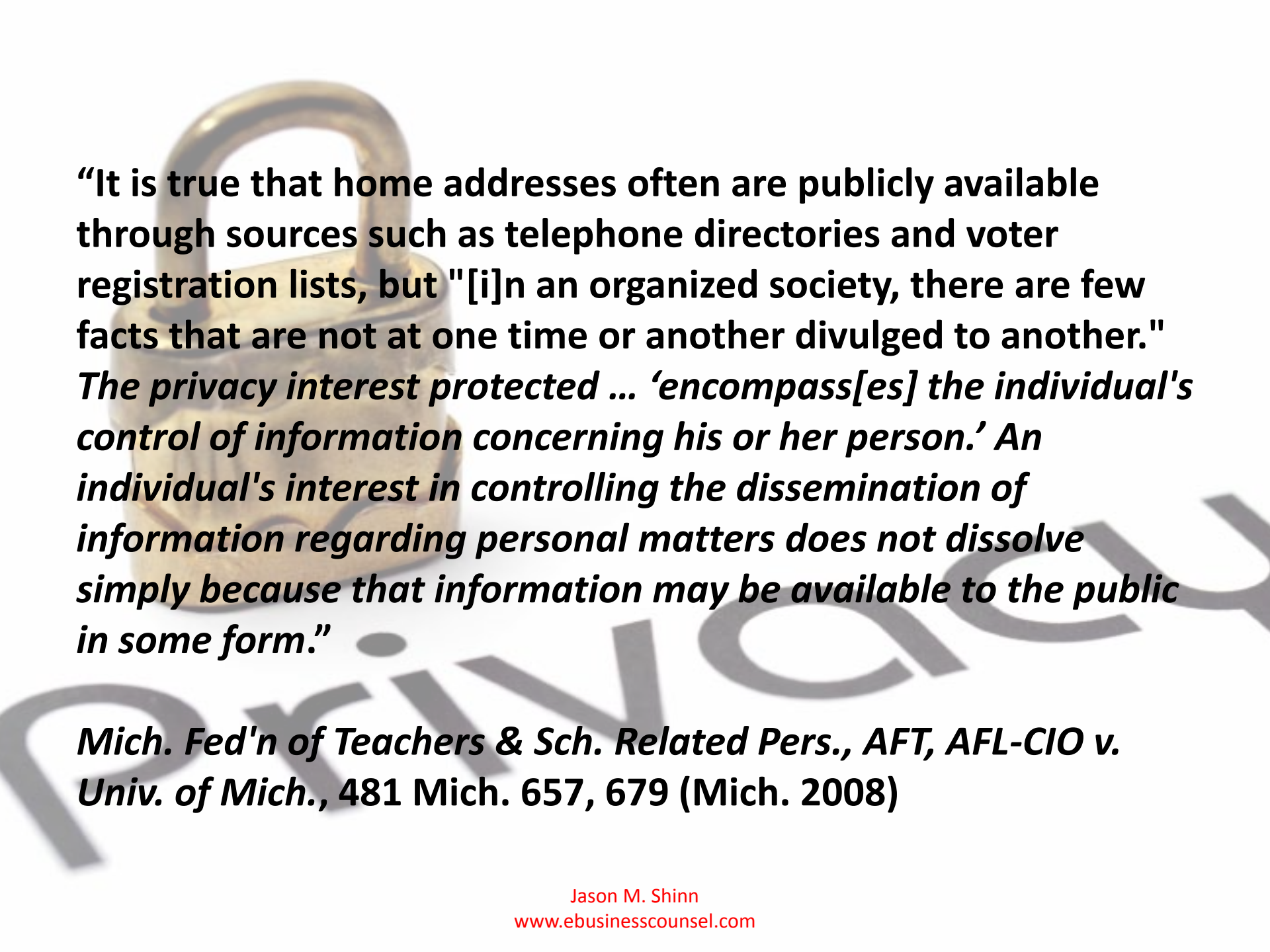
Privacy & Data Breach In the Headlines

- **Aaron's Rental Co.'s Laptops Track Users' Keystrokes and Screenshots, Take Webcam Photos (5/3/2011)**
- **Citigroup Cites \$2.7 Million in Customer Losses From Breach (6/25/2011)**
- **Study: Organizational Data Breach Costs Hit \$7.2 Million and Show No Sign of Leveling Off (3/8/2011)**
- **Inside the Anonymous Army of 'Hacktivist' Attackers (6/23/2011)**
- **ACLU Calls Background Checks Asking for Social Network Passwords of Job Applicants Illegal Invasion of Privacy (2/22/2011)**
- **No Criminal Charges in Case Over School District's Alleged Webcam Spying on Students (8/17/2010)**

Privacy Right Origins

“The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others. . . . [E]ven if he has chosen to give them expression, he generally retains the power to fix the limits of the publicity which shall be given them.”

Warren & Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 198 (1890-1891)



“It is true that home addresses often are publicly available through sources such as telephone directories and voter registration lists, but “[i]n an organized society, there are few facts that are not at one time or another divulged to another.”
The privacy interest protected ... ‘encompass[es] the individual's control of information concerning his or her person.’ An individual's interest in controlling the dissemination of information regarding personal matters does not dissolve simply because that information may be available to the public in some form.”

Mich. Fed'n of Teachers & Sch. Related Pers., AFT, AFL-CIO v. Univ. of Mich., 481 Mich. 657, 679 (Mich. 2008)



Instagram



LinkedIn

my

Myspace



Skype



Messenger



Facebook



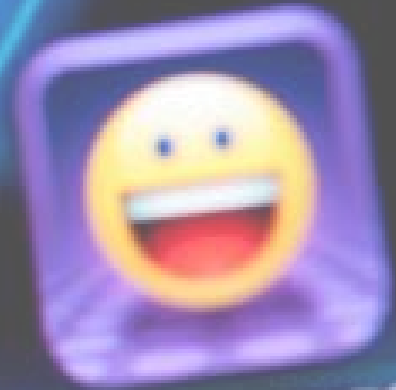
Twitter



foursquare



viber



Y! Messenger

What Protections Should be Extended to Privacy?

- **Use without permission?**
- **Expectation of privacy?**
- **Information Falling into wrong hands?**
- **Erosion of anonymous information?**
- **Assembling information into specific profiles?**

Overview of Regulatory Landscape of Information Protection

- Children's Online Privacy Protection Act
- Federal Trade Commission (FTC)
- State Laws
- Gramm-Leach Bliley Act
- Sarbanes-Oxley Act
- International Standards
- Federal Privacy Act
- Government Information Security Reform Act
- Federal Information Security Management Act (FISMA)
- Payment Card Industry Security Standards Council, or PCI SSC
- Fair Credit Reporting Act ("FCRA")
- Litigation

Jason M. Shinn

www.ebusinesscounsel.com

Civil Claims for Data Breaches

- Plaintiffs have generally been unable to persuade courts of their injury or prove damages merely based upon the unauthorized theft or loss of their personal information.
- Courts generally take the view that an increased risk of future injury from identity theft exposure is insufficient to support an actionable injury or to establish damages.
- Failing to show a causal connection between the defendant's actions and the plaintiff's alleged injury is another hurdle in establishing standing or showing damages in security breach cases..

State Security Breach Notification Laws

- Alaska, Alaska Stat. § 45.48.010 et seq.
- Arizona, Ariz. Rev. Stat. § 44-7501
- Arkansas, Ark. Code § 4-110-101 et seq.
- California, Cal. Civ. Code §§ 56.06, 1785.11.2, 1798.29, 1798.82
- Colorado, Colo. Rev. Stat. § 6-1-716
- Connecticut, Conn. Gen Stat. 36a-701(b)
- Delaware, Del. Code tit. 6, § 12B-101 et seq.
- Florida, Fla. Stat. § 817.5681
- Georgia, Ga. Code §§ 10-1-910, -911
- Hawaii, Haw. Rev. Stat. § 487N-2
- Idaho, Idaho Stat. §§ 28-51-104 to 28-51-107
- Illinois, 815 ILCS 530/1 et seq.
- Indiana, Ind. Code §§ 24-4.9 et seq., 4-1-11 et seq.
- Iowa, Iowa Code § 715C.1
- Kansas, Kan. Stat. 50-7a01, 50-7a02
- Louisiana, La. Rev. Stat. § 51:3071 et seq.
- Maine, Me. Rev. Stat. tit. 10 §§ 1347 et seq.
- Maryland, Md. Code, Com. Law § 14-3501 et seq.
- Massachusetts, Mass. Gen. Laws § 93H-1 et seq.
- Michigan, Mich. Comp. Laws § 445.72
- Minnesota, Minn. Stat. §§ 325E.61, 325E.64
- Mississippi, 2010 H.B. 583 (effective July 1, 2011)
- Missouri, Mo. Rev. Stat. § 407.1500
- Montana, Mont. Code §§ 30-14-1704, 2-6-504
- Nebraska, Neb. Rev. Stat. §§ 87-801-807
- Nevada, Nev. Rev. Stat. 603A.010 et seq.
- New Hampshire, N.H. Rev. Stat. §§ 359-C:19, -C:20, -C:21
- New Jersey, N.J. Stat. 56:8-163
- New York, N.Y. Gen. Bus. Law § 899-aa
- North Carolina, N.C. Gen. Stat § 75-65
- Ohio, Ohio Rev. Code §§ 1347.12, 1349.19, 1349.191, 1349.192
- Oklahoma, Okla. Stat. § 74-3113.1 and § 24-161 to -166
- Oregon, Oregon Rev. Stat. § 646A.600 et seq.
- Pennsylvania, 73 Pa. Stat. § 2303
- Rhode Island, R.I. Gen. Laws § 11-49.2-1 et seq.
- South Carolina, S.C. Code § 39-1-90
- Tennessee, Tenn. Code § 47-18-2107, 2010 S.B. 2793
- Texas, Tex. Bus. & Com. Code § 521.03
- Utah, Utah Code §§ 13-44-101, -102, -201, -202, -310
- Vermont, Vt. Stat. tit. 9 § 2430 et seq.
- Virginia, Va. Code § 18.2-186.6, § 32.1-127.1:05
- Washington, Wash. Rev. Code § 19.255.010, 42.56.590
- West Virginia, W.V. Code §§ 46A-2A-101 et seq.
- Wisconsin, Wis. Stat. § 134.98 et seq.
- Wyoming, Wyo. Stat. § 40-12-501 to -502
- District of Columbia, D.C. Code § 28-3851 et seq.
- Puerto Rico, 10 Laws of Puerto Rico § 4051 et. seq.
- Virgin Islands, V.I. Code § 2208

States with no security breach law: Alabama, Kentucky, New Mexico, and South Dakota.



Jason M. Shinn

www.ebusinesscounsel.com

Data Breach Notification Obligations



- **Information Protected** - Statutes generally apply to unencrypted sensitive personally identified information - e.g., information consisting of first name or initial and last name, plus one of the following: social security number, drivers license or other state ID number, or financial account number or credit or debit card number (along with any PIN or other access code where required for access to the account).
- **Definition of breach** - Statutes generally require notice following the unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of such personal information. In some states, however, notice is not required unless there is a reasonable basis to believe that the breach will result in substantial harm or inconvenience to the customer.

Data Breach Notification Obligations



- **Notification** - Notice must be given to any residents of the state whose unencrypted personal information was the subject of the breach.
- **Timing of Notice** - Generally, persons must be notified in the most expedient time possible and without unreasonable delay; however, in most states the time for notice may be extended for the following:
 - Legitimate needs of law enforcement, if notification would impede a criminal investigation
 - Taking necessary measures to determine the scope of the breach and restore reasonable integrity to the system

Data Breach Notification Obligations



- **Form of notice** - Notice may be provided in writing (e.g., on paper and sent by mail), in electronic form (e.g., by e-mail, but only provided the provisions of E-SIGN are complied with), or by substitute notice.
- **Substitute notice options** - If the cost of providing individual notice is greater than a certain amount (e.g., \$250,000) or if more than a certain number of people would have to be notified (e.g., 500,000), substitute notice may be used, consisting of:
 - E-mail when the e-mail address is available, and
 - Conspicuous posting on the company's web site, and
 - Publishing notice in all major statewide media.

Michigan Data Breach Notification Statute



- Notification limited to determination that breach has not or is not likely to cause “**substantial loss or injury to, or result in identity theft**” with respect to, one or more Michigan residents:
- Does not apply to encrypted data, *unless* there was unauthorized access to the encryption key.
- Key Questions:
 - Does trigger for notification create too high a bar?
 - Does lower bar risk desensitization?
 - What obligations to **out of state residents?**

Cost of Data Breaches

- **The average cost of a data breach increased by seven percent to \$7.2 million in 2010, with the cost of each compromised record now averaging \$214, up from \$209 in 2009.**
- **Costs of a data breach include notification and legal defense costs, penalties from regulations such as the HITECH Act, and lost customer business.**
- **For the first time, malicious or criminal attacks are the most expensive cause of data breaches and not the least common one; up from 12% in 2008, to 24% in 2009, to 31% in 2010.**
- **Quick responses to data breaches are more costly than slower responses – 54% more, to be precise. With the haste to comply with state and federal regulations, some companies rush to get the notification process over with, and in the process over-notify more than needed.**
- **Companies are more proactively protecting themselves from data breach threats. For example, breaches due to systems failures, lost devices and third-party mistakes are lower than before. And while some companies may be responding to breaches too hastily (and inefficiently), the good news is that more companies are responding to breaches within 30 days of an incident.**

What are Businesses to Do?



Best Practices for Businesses

Risk Management - Data Security practices

- **Assess what information is possessed**
- **Retain only what serves business/legal purpose**
- **Secure information**
- **Proper disposal methods**
- **Plan for breach**
- **Educating records custodians and employees**

Best Practices for Businesses

Public Relations

- Use info to provide best possible product and services
- Develop innovative products/services that reflect strong privacy standards and practices
- Make collection of information transparent
- Give users meaningful choices
- Be responsible stewards of data





Since 2011, Jason Shinn has collaborated with businesses on all aspects of e-commerce and Internet law, including securing and protecting website content and complying with specific Internet laws and regulations (e.g., CAN-SPAM, DMCA, COPPA, FTC regulations, and privacy regulation compliance). He also provides employment law/human resource counseling to address day-to-day employment matters, responding to agency charges, and litigating these issues in state and federal courts. Mr. Shinn has also lead internal investigations involving compromised company information of consumer, employee, and company data.