

**Miami Valley Computing Societies
17th Annual Fall Joint Meeting**

Monday, September 26, 2005

David H. Ponitz Center

Sinclair Community College

Who's Watching You(r Data)

Protection through Best Practices,
Contracts, and Legislation

Dino Tsibouris
dino.tsibouris@mt-law.com
www.mt-law.com
(614) 228-9707 Ext. 12

Federal Privacy Law

- FERPA - Education
- Bank Secrecy Act
- Gramm Leach Bliley - Financial
- HIPAA – Health information
- FTC Act

State Privacy Law

- California – Website privacy statement law
- Vermont – Financial data sharing
- California – Data protection
- Common law right to privacy or publicity

State Privacy Law - Ohio

- On August 2, 2005, the Ohio House passed House Bill 104.

To ... require a state agency, person, or business to contact individuals residing in Ohio if unencrypted or unredacted personal information about those individuals that is maintained on the computers of the agency, person, or business is obtained by unauthorized persons and to authorize the Attorney General to investigate and enforce compliance with the requirements.

International Privacy Law

- Canada
- European Directive
- Offshoring

IT Contracts - Privacy

- Confidentiality agreements
- Outsourcing and data processing contracts
- Website privacy statements and terms of use

IT Contracts - Privacy

- Each party shall take all reasonable steps to assure that any material or information considered by either party to be confidential which has or will come into the possession or knowledge of each in connection with this Agreement, whether transmitted prior to or after the effective date of this Agreement, shall not be disclosed to others, in whole or in part, without the prior written permission of the other party, and shall be used solely for the purpose for which such material or information was provided and for no other purpose whatsoever.

IT Contracts - Privacy

- Black's Law Dictionary defines "reasonable" as "[fair, proper, just, moderate, suitable under the circumstances. Fit and appropriate to the end in view."
- Unless the term "reasonable steps" is defined to mean "that which is customarily practiced in the industry" or in some other verifiable way, the standard is not objectively defined.



Incident Management

- Brazos Student Lending – Employee laptop stolen
- Wells Fargo – Laptop lost
- Citibank – Data tape lost

Incident Management

Details emerge on credit card breach

Mon. Jun 20 16:51:00 PDT 2005; News.com

Exposed more than 40 million credit card accounts to fraud.

- Intruders exploited software security vulnerabilities to install a rogue program on the network of CardSystems Solutions, MasterCard International spokeswoman Jessica Antle said. The program captured credit card data, she said.
- Malicious code discovered after a probe into the security of CardSystems' network, triggered by a MasterCard inquiry into atypical reports of fraud by several banks.
- Cardsystems did not meet MasterCard's security regulations and retained records it should have discarded, and stored transaction data in unencrypted form.

Incident Management

- FTC Guidance
- Law Enforcement
- Notification
- Contract administration and indemnity
- Litigation

Enforcement – State AG (Ohio)

- **Attorney General Petro Sues DSW Over Customer Data Theft. June 6, 2005 (COLUMBUS)**
- Attorney General Jim Petro today asked a court to order Ohio-based shoe retailer Designer Shoe Warehouse (DSW, INC.) to individually notify each customer whose personal information may have been stolen recently from DSW computer files. Ohio is the first state to sue the retailer over one of the biggest security breaches of its kind in the nation.
- www.ag.state.oh.us/press_releases/2005/pr20050606.htm

Enforcement – State AG (NY)

- **VICTORIA'S SECRET SETTLES PRIVACY CASE.** Oct 21, 2003 –
- "A business that obtains consumers' personal information has a legal duty to ensure that the use and handling of that data complies in all respects with representations made about the company's information security and privacy practices," Spitzer said.

Enforcement – State AG (NY)

- **VICTORIA'S SECRET SETTLES PRIVACY CASE.** Oct 21, 2003
- Privacy policy: "Any information you provide to us at this site when you establish or update an account, enter a contest, shop online or request information . . . is maintained in private files on our secure web server and internal systems . . ."
- Despite that, consumers' personal information, including name, billing address, and items ordered, was available on the company web site for four months ending in late November of 2002.
- http://www.oag.state.ny.us/press/2003/oct/oct21b_03.html

How to Protect Yourself

- Pay retail and online with a credit card or cash
- Don't mail your bills from your home mail box
- Read your billing statements promptly and carefully
- Pay bills using online bill pay

How to Protect Yourself

- Place a fraud alert on your credit report
- Close the accounts that you know or believe have been tampered with or opened fraudulently
- File a report with your local police or the police in the community where the identity theft took place
- Contact Attorney General or FTC
- <http://www.consumer.gov/idtheft/>

SPAM

- CAN SPAM Act
- Ohio Revised Code § 2307.64. Electronic mail advertisements

Spyware

- Spyware - programs that monitor user activities, and transmit user information to remote servers and/or show targeted advertisements
- Adware - Software application in which advertising banners are displayed while the program is running

Lawsuits

- Direct Revenue – March 2005
- Intermix - \$7.5 million penalty (Spitzer)
- Claria - Settled
- WhenU - Settled
- 180Solutions - Settled

Legislation - Federal

- Safeguard Against Privacy Invasions Act - Rep. Mary Bonq - H.R. 29 Passed House, May 23, 2005.
 - Requires notice, consent, and uninstall capability for information collection and advertising programs
 - Prohibits certain practices without consent. Enforcement by the FTC
 - Preempts existing statespyware laws

Legislation - Federal

- Internet Spyware (I-SPY) Prevention Act - Rep. Bob Goodlatte - Passed House, May 23, 2005.
 - Creates criminal penalties for accessing a protected computer without authorization, or exceeding authorization, by causing software to be copied onto a computer and 1) using that code for another Federal criminal offense, 2) intentionally obtaining or transmitting personal information with intent to defraud, injure, or cause damage, or 3) intentionally impairing computer security.

Legislation - State

- Legislation is being considered in at least 28 states in 2005. Legislation has been enacted in nine states: Arizona, Arkansas, Georgia, Iowa, New Hampshire, Texas, Utah, Virginia and Washington.

Questions?