



MBA's NATIONAL TECHNOLOGY IN
MORTGAGE BANKING CONFERENCE & EXPO
APRIL 25-28, 2010, HYATT REGENCY CHICAGO

Recent Developments in Information Privacy and Security Laws and Regulations

Panelists:

Bruce H. Nielson, Partner, K&L Gates

Paul H. Luehr, Managing Director and General Counsel, Stroz Friedberg

Andrew M. Smith, Partner, Morrison & Foerster

Henry L. Judy, Of Counsel, K&L Gates

- Introduction of Panelists
- Why this Topic?
- Presentation Overview
 - Data Breach Response: A Practical Approach (Paul Luehr)
 - State Information Security Requirements (Bruce Nielson)
 - Federal Identity Theft Laws and Rules (Andrew Smith)
 - Developments at the Edge, and Beyond (Hank Judy)
- Format for each of these four presentations will be: Presentation, Audience Questions, Panel Discussion

- **Headline: 22 Banking Breaches So Far in 2010** (bankinfosecurity.com, 3/22/10)
 - 173 total reported data breaches so far in 2010
 - 22 involved financial services companies
 - 62 banking-related breaches reported in all of 2009
 - Numbers include banks, mortgage banks, mortgage brokers, securities firms, payment processors, etc.
 - “Despite the Federal Trade Commission's work in promoting the ID Theft Red Flags Rule, . . . many businesses still don't want to comply with the requirements. ‘If you don't want to protect it, then don't collect the data’”
 - “For those organizations that do buy into data protection, they must deputize their employees to take the responsibility seriously. ‘You should be telling your employees why it is important, so they buy into the wanting to actively protect data, and so they don't see it as another chore’”

- State Lawmakers/Regulators Are Not Standing Idly By . . .
 - State Data Breach Notification and Remediation Requirements
 - On April 7, 2010, Mississippi became the 46th state to enact a data security breach notification law; the law goes into effect July 1, 2011
 - Now only four states (Alabama, Kentucky, New Mexico and South Dakota) do not have a data security breach notification law
 - Some states have adopted or are considering tough and specific personal information security requirements, such as Massachusetts

- . . . And Neither Are Their Federal Counterparts . . .
 - Federal identity theft rules, including the FTC's Red Flags Rule
 - ID theft rules are in addition to the federal GLB and HIPAA laws and regulations – including the banking regulators' Interagency Guidelines Establishing Standards for Safeguarding Customer Information and the SEC's proposed, but never finalized, information security revisions to its Regulation S-P
 - Enforcement by federal agencies, including the FTC, SEC, and bank regulators
 - The FTC announced on March 25, 2010 that it had entered into a settlement with a company in the agency's "27th case challenging faulty data security practices by organizations that handle sensitive consumer information"
 - Commerce Department announced April 21, 2010 that it seeks comments on questions related to the adequacy of U.S. privacy policies in light of the growth of online commerce – comments due by June 7
 - Is the "notice and choice" approach to consumer data privacy still a useful model?
 - What hurdles do businesses face in complying with different state laws concerning privacy and data protection?
 - What hurdles do businesses face in complying with different foreign laws concerning privacy and data protection?
 - How does the current sectoral approach to privacy regulation affect consumer experiences, business practices, or the development of new business models?

- . . . Nor Are Self-Regulatory and Industry Organizations
 - The Financial Industry Regulatory Authority (FINRA) announced on April 12, 2010 a fine of \$375,000 against a securities broker-dealer for its “failure to protect confidential customer information by allowing an international crime group to improperly access and hack the confidential information of approximately 192,000 customers”
 - The Payment Card Industry Data Security Standards (PCI DSS) were substantially strengthened with the release of PCI DSS Version 1.2 in October 2008 (since updated to Version 1.2.1)

- The Risks to Information Privacy and Security Are Increasing with Advancing Technologies and Applications
 - As data transmittal, processing, storage and transaction devices get smaller (notepads, Iphones, Ipads, cell phones, Blackberry devices, thumb drives, etc.) and/or “smarter” (photocopiers, swipe cards, card readers, etc.), the risks of loss or theft of data increases
 - A survey from 2009 in the UK found that 4,500 USB memory sticks were left in pockets of clothes sent to dry cleaners
 - Use of social media networks by and within enterprises (Facebook, MySpace, Twitter, LinkedIn, Blogs, etc.)



MBA's NATIONAL TECHNOLOGY IN
MORTGAGE BANKING CONFERENCE & EXPO
APRIL 25-28, 2010, HYATT REGENCY CHICAGO

Data Breach Response: A Practical Approach

Presented by:

Paul Luehr, Managing Director

pluehr@strozfriedberg.com

612-605-3000

STROZ FRIEDBERG

2009 Average Loss to Organization = \$6.75 million

- » Highest = \$31 million

- » Lowest = \$750,000

2009 Average Loss per Victim = \$204

- » Cost per Malicious Attack = \$215

- » Cost per Negligent Employee = \$154

2009 Malicious Attacks Doubled

- » Up from 12% to 24% of Total

Source: Ponemon Institute/PGP Corp., 2009 Annual Study: Cost of a Data Breach (45 organizations surveyed across 15 sectors)

PREPARE

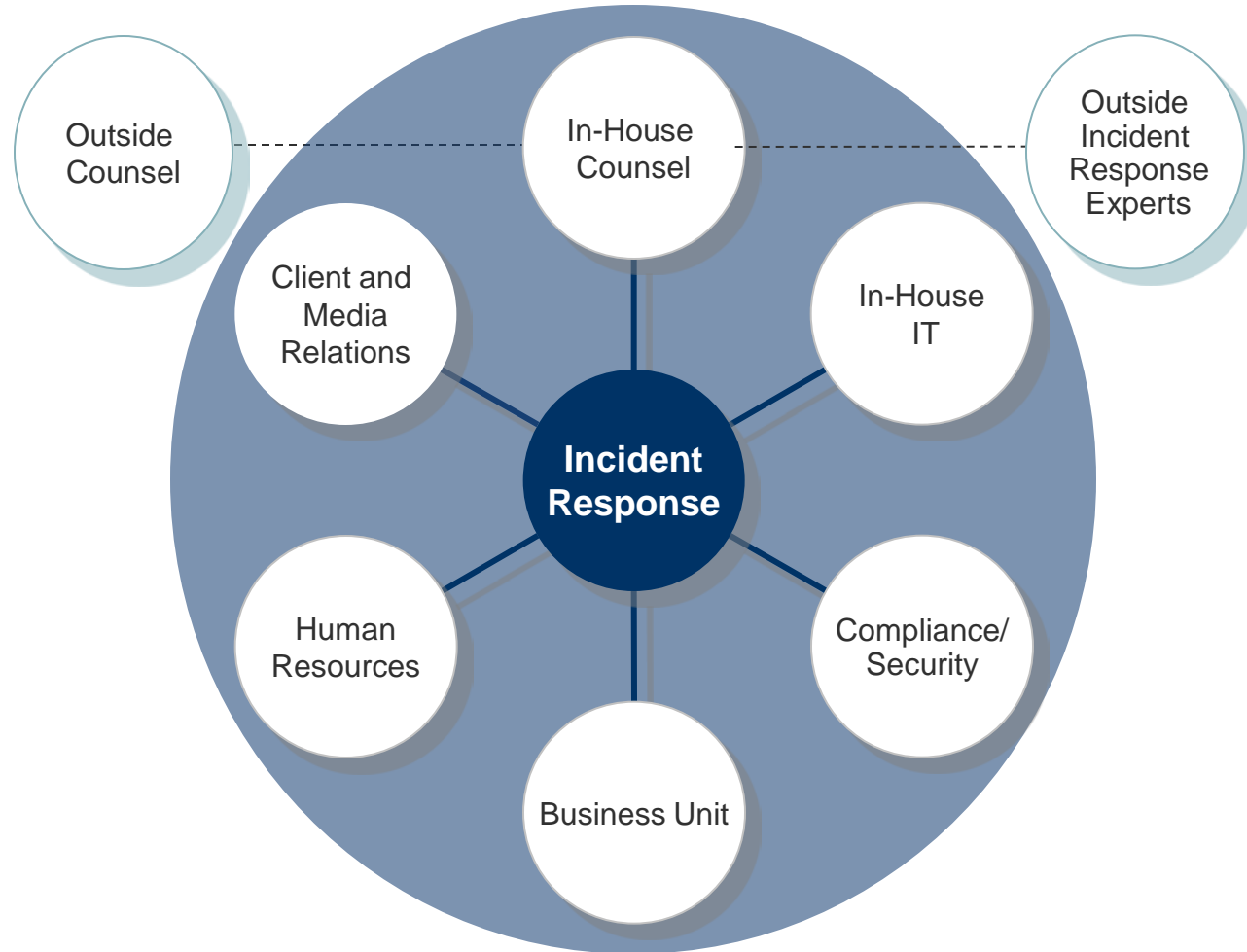
PRESERVE

ASSESS

SEARCH

NOTIFY

PREPARE: Build your Team



Map your critical assets

Record backup schedules and inventories

Update user lists

Centralize logging functions

Synchronize network times

Include:

Management endorsement

Contact lists

Legal analysis and timeline

Categories of adverse events

“First steps” checklists

Facilities and equipment list

Outreach plan

PRESERVE: the Data

Unhook infected machines (leave power on).

- » Do **NOT** poke around.
- » Insert clean and patched machines.

Call forensic experts to image infected machines.

Save off log files (e.g. web, firewall, IDS).

Pull backup tapes out of rotation.

Save keycard data and surveillance tapes.

Start real-time packet capture.

Force password change.



Physical Steps

HR Steps

Technical Steps

Legal Steps

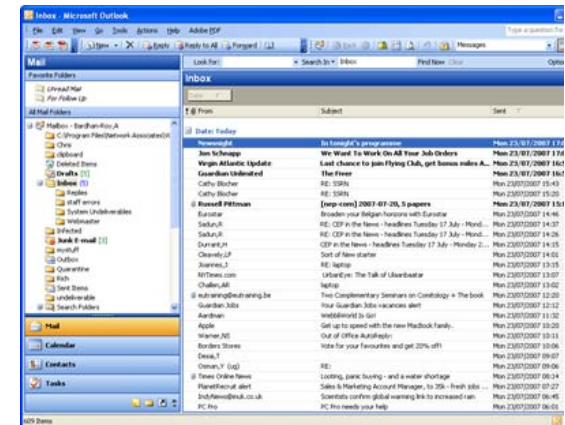
Overall Goal – to determine:

- » If data has really been lost or compromised
- » Type of PII that's been compromised
- » Time period of breach
- » Initial volume estimate

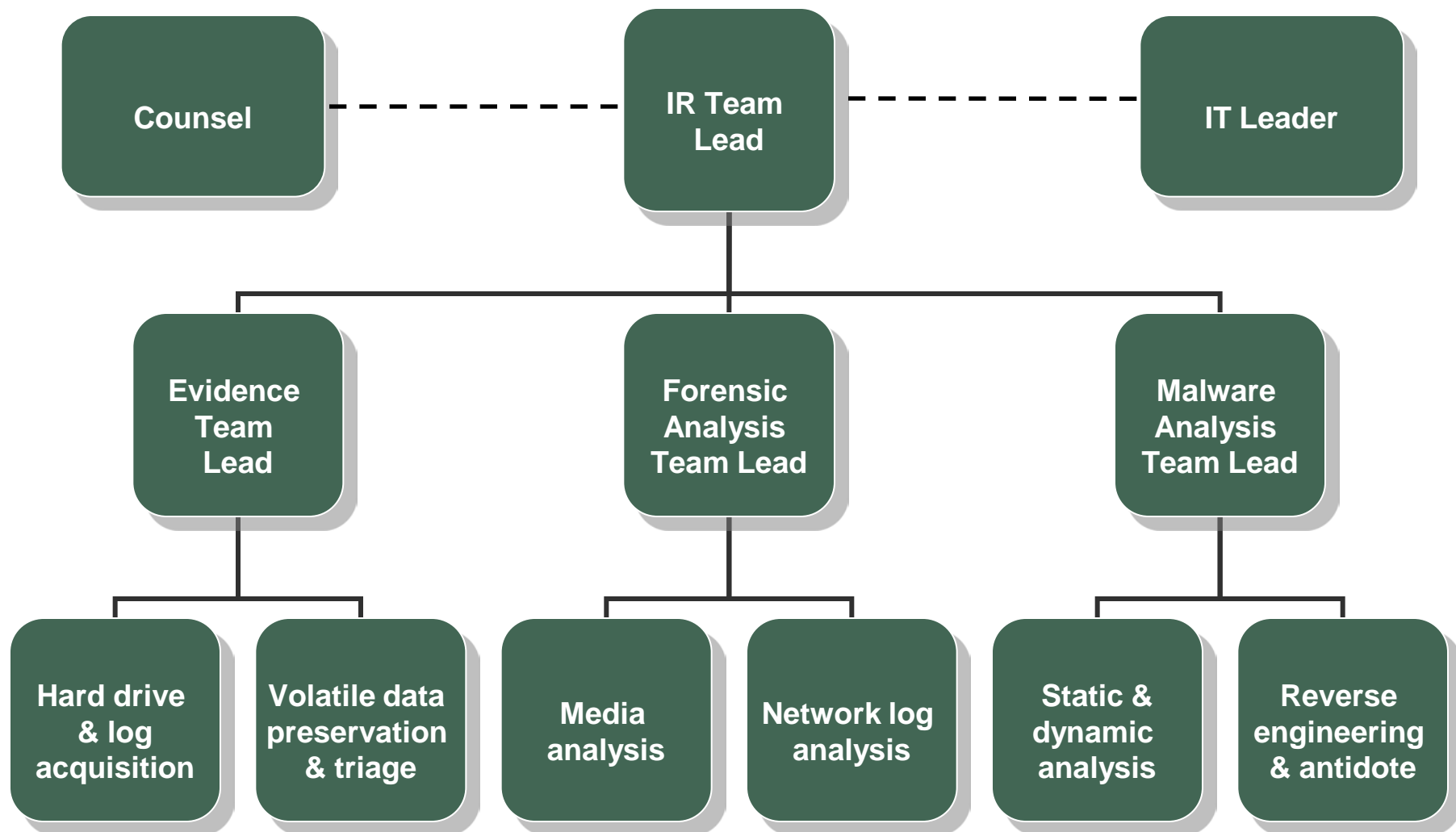
ASSESS: Technical Steps

Are there other data sources that may reflect the contents of the lost data?

How closely do the available data sources resemble the lost data?



Technical Incident Response Team

















ASSESS: Forensic Steps

Proc#	PPID	PID	Name:
0	0	0	Idle
1	0	8	System
2	8	156	smss.exe
3	144	164	winlogon.exe
4	144	168	csrss.exe
5	156	176	winlogon.exe
6	156	176	winlogon.exe
7	156	180	csrss.exe
8	176	228	services.exe
9	176	240	lsass.exe
10	1112	284	dd.exe
11	820	324	helix.exe
12	228	408	svchost.exe
13	228	436	spoolsv.exe
14	228	464	Avsynmgr.exe
15	228	480	svchost.exe
16	228	540	regsvc.exe
17	228	552	MSTask.exe
18	228	592	dfnws2005.exe
19	464	612	VsStat.exe
20	464	628	Avconsol.exe
21	600	668	UMGR32.EXE
22	228	672	WinMgmt.exe
23	800	820	Explorer.Exe
24	820	964	Apoint.exe
25	820	972	HKserv.exe
26	820	972	HKserv.exe
27	820	988	DragDrop.exe
28	820	1008	alogserv.exe
29	820	1012	tgcmd.exe
30	820	1048	PcfMgr.exe
31	408	1064	JogServ2.exe
32	864	1072	Apntex.exe
33	820	1076	cmd.exe
34	592	1096	nc.exe
35	324	1112	cmd2k.exe

Volatile Data Capture

Capturing physical memory may reveal processes not normally seen by user or IT.

DELETED FILES: Hacker's Toolkit

Name+	Type	Modified	Size
 EraseLog.vbs+	VBScript Script File	7/9/2005 4:20 PM	1,109
 FindPass.exe+	Application	3/4/2005 11:37 AM	17,408
 Letmein.exe+	Application	12/30/2005 3:24 PM	18,432
 ListAdmins.vbs+	VBScript Script File	7/12/2005 5:45 PM	1,213
 Netsvc.exe+	Application	12/25/2005 12:07...	14,336
 NETVIEWX.EXE+	Application	9/4/2002 12:09 PM	40,960
 Psexec.exe+	Application	9/4/2002 12:09 PM	90,112
 PsKill.exe+	Application	3/8/2004 1:01 PM	26,624
 Psloggedon.exe+	Application	9/6/2002 4:43 PM	45,056
 pspasswd.exe+	Application	5/16/2004 8:36 AM	57,344
 Pulist.exe+	Application	9/6/2002 11:34 AM	55,296
 rasmon.dll+	Application Extension	12/30/2005 3:24 PM	4,608
 rasmon.exe+	Application	12/30/2005 3:24 PM	16,384
 Sqlrcmd.asp+	ASP File	8/25/2002 7:03 PM	4,004

Use law as your guide; focus on PII, PHI.

Conduct sample searches.

Determine level of acceptable accuracy.

Account for variations but be consistent.

Electronic Searches – look for:

- » Numerical Sequences, e.g. SSN and Credit Card Numbers
- » PII-related Keywords
- » Record Identifiers that May Contain PII
- » “Unsearchable” images
- » Embedded files

Name (first initial, last), PLUS

(Address - Street, Internet)

Date of birth (DOB)

Telephone number (home, cell)

Account identifier

» Account number

» Credit card number

» Debit card number

Access codes (e.g. usernames and passwords)

Government identifier

» Social Security number

» Driver's license

Social security number:

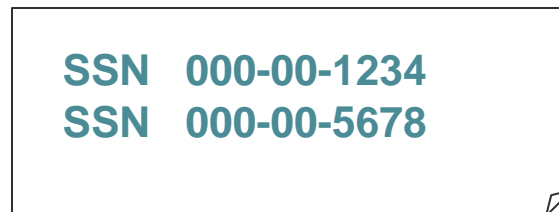
=== - == - =====, === == =====, =====,

“SSN, Social Security Number, socsec,” etc.

Credit card number:

5411222233334444 = 5.41122E+15 in binary

Unsearchables:



SSN 000-00-1234
SSN 000-00-5678

SEARCH: Use Advanced E-Discovery Tools



- 007-DOJ-AG [Doc No in Box: 1 of 102]
- DOCTYPE INFO
 - DOCTYPE
 - EDOC
 - T_DOCTYPE
 - email
- DOCDATE INFO
 - DOCDATE
 - 1980/01/12
 - T_DOCDATE**
 - 2005/02/18
- TITLE INFO
 - TITLE
 - DOJDocsPt1070009.PDF
 - T_TITLE
 - RE: 2 AGAC items
- AUTHORS
 - AUTHOR
 - RENATA
 - T_AUTHORNAME
 - Sampson, Kyle
- RECIPIENTS
 - T_RECIPNAME
 - Mercer, Bill
- T_EMAILADDRESS
 - Judy.Beeman2@usdoj.gov
 - Kyle.Sampson@USDOJ.gov
- T_ORGANIZATION
 - Legislative Committee
- T_PERSON
 - Beeman, Judy
 - Gonzales
 - Mercer, Bill
 - Sampson, Kyle
 - Ulylot, Ted
- OTHER DATES INFO
 - T_OTHER_DATES**
 - 2005/02/17
 - 2005/02/18
 - 2005/03/02

Extracts text from the face of the document and organizes the information

Sampson, Kyle

From: **Sampson, Kyle**
Sent: **Friday, February 18, 2005 8:23 AM**
To: Mercer, Bill
Subject: RE: 2 AGAC items

ok, good
will look for recommendations from you on subcommittees

-----Original Message-----
From: Mercer, Bill
Sent: **Thursday, February 17, 2005 10:41 PM**
To: Sampson, Kyle
Subject: Re: 2 AGAC items

would have a conversation about the subcommittees.

are doing well. I would like to add a Legislative
to interact w/OLA and OLP. I would recommend termination of
I don't see this as a core function at this
We don't have much of a budget. I can't see the value in this one.

leaves
/Immigration (Iglesias):
/reconstituted. These are a mixed bag. Some are the least active and should get new

as these decisions are made, I will let people know that now is the time to
add/leave subcommittees.

-----Original Message-----
From: Sampson, Kyle <Kyle.Sampson@USDOJ.gov>
To: Mercer, Bill <Bill.Mercer@usdoj.gov>
Cc: **Beeman Judy, Judy.Beeman2@usdoj.gov**
Sent: Thu Feb 17 17:24:56 2005
Subject: 2 AGAC items

A couple of AGAC items:

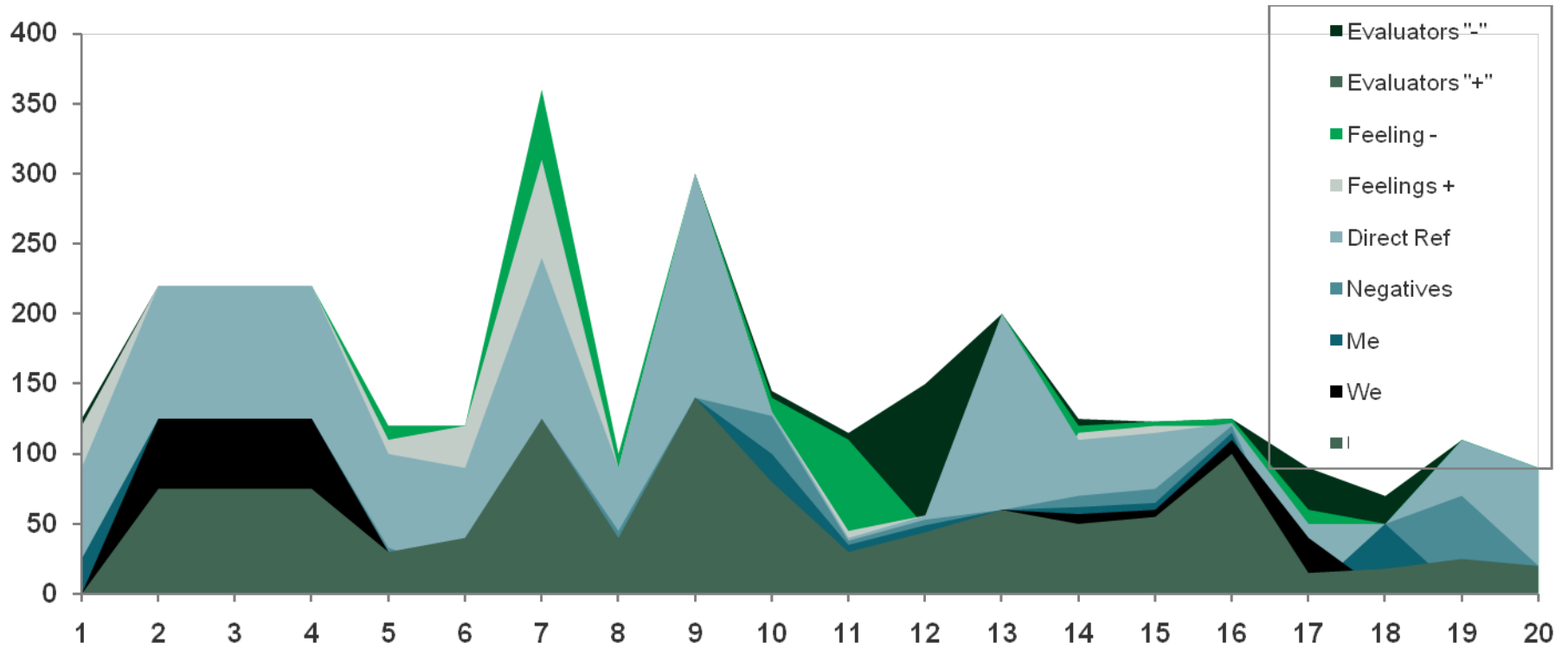
1. The Attorney General would like to have dinner with the AGAC on the evening of **Wednesday, March 2, 2005** beginning at approximately 6pm (or 6:30pm)? Could you all select a restaurant and make reservations and add to the AGAC schedule of events? Participants would be USAs, AG (and perhaps Mrs. Gonzales), me, and Ted Ulylot.
2. The Attorney General would like to make the following appointments to the AGAC:
appointments (for terms expiring **12/31/2007**)

“His experience was **ZERO**. He does **not** know **ANYTHING** about ...our reporting tools.

“Until you **fire me** or I **quit**, I have to take orders from you...Until he is a trained expert, I **won't** give him access...If you order **me** to give him root access, then you have to **permanently relieve me** of my duties on that machine. I **can't** be a **garbage cleaner** if someone **screws up**....I won't compromise on that.”

- Content Analysis Cues
 - **Negatives/anger**
 - Me/victimization
 - **Key word/risk behavior**

Indicators of Anger (+)



Scope of Notifications - multiple parties to consider

Victims (customers v. employees)

Business partners (CRAs, VISA, processors, realtors)

Regulators

Even the media

» HITECH Act: notice to “prominent media outlets” if victims > 500

Time Frames - vary by jurisdiction and law

“Without unreasonable delay” CA, NY, MN, HHS, FTC

45 days, OH, FL

60 days, HITECH Act and DATA bill

Questions?

Paul Luehr

Stroz Friedberg



MBA's NATIONAL TECHNOLOGY IN
MORTGAGE BANKING CONFERENCE & EXPO
APRIL 25-28, 2010, HYATT REGENCY CHICAGO

State Information Security Requirements

Bruce H. Nielson, Partner (Washington DC Office)

bruce.nielson@klgates.com

202-778-9256

K&L | GATES

- California

- “A business that owns or licenses 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.” Cal. Civ. Code § 1798.81.5(b), enacted in 2004
- “A business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party shall require by contract that the third party 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.” § 1798.81.5(c)
- “Personal information” is defined as “an individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: (A) Social security number; (B) Driver's license number or California identification card number; (C) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (D) Medical information.” § 1798.81.5(d)

- Rhode Island

- “A business that owns or licenses computerized unencrypted personal information about a Rhode Island 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,” Gen. Laws of Rhode Island § 11-49.2-2(2), enacted in 2005

- Texas

- “A business shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business.” Texas Bus. & Comm. Code § 48.102(a), effective Sept. 1, 2005
- A proposed amendment to this section would make the PCI DSS standards applicable to all businesses that collect or store “sensitive personal information” in connection with transactions involving credit, debit or stored value cards issued by financial institutions and would give financial institutions the ability to sue businesses that have data security breaches and did not comply with PCI DSS standards

- Oregon
 - Any person that owns, maintains or otherwise possesses data that includes a consumer's personal information that is used in the course of the person's business, vocation, occupation or volunteer activities must develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the personal information," Oregon Rev. Stat. § 646A.622(1), enacted July 2007, effective Jan. 1, 2008
- Nevada
 - "A business in this State shall not transfer any personal information of a customer through an electronic transmission other than a facsimile to a person outside of the secure system of the business unless the business uses encryption to ensure the security of electronic transmission." Nev. Rev. Stat. § 597.970(1), effective Oct. 1, 2008

- Connecticut

- “Any person in possession of personal information of another person shall safeguard the data, computer files and documents containing the information from misuse by third parties, and shall destroy, erase or make unreadable such data, computer files and documents prior to disposal.” Conn. Pub. Act 08-167 § 1(a), effective October 1, 2008
- “Personal information” defined as “information capable of being associated with a particular individual through one or more identifiers, including . . . a Social Security number, a driver's license number, a state identification card number, an account number, a credit or debit card number, a passport number, an alien registration number or a health insurance identification number”

- Massachusetts
 - “Standards for the Protection of Personal Information of Residents of the Commonwealth,” Mass. Reg. 201 CMR 17.00, effective March 1, 2010
 - Contains detailed (onerous?) information security program requirements
- Application and Scope of Massachusetts Regulation
 - Regulation applies to “every person that owns or licenses personal information about a resident” of Massachusetts
 - “Owns or licenses” means “receives, stores, maintains, processes or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment”
 - “Person” is defined to include natural persons, corporations, associations, partnerships and other legal entities
 - “Personal information” is defined as “a Massachusetts resident’s first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver’s license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password. that would permit access to a resident’s financial account”

- Overview of Massachusetts Regulation:
 - Two main substantive sections:
 - Duty to develop and implement a “comprehensive, written information security program” (WISP) that “contains administrative, technical and physical safeguards that are appropriate to (a) the size, scope and type of business of the person obligated to safeguard the personal information . . . ; (b) the amount of resources available to such person; (c) the amount of stored data; and (d) the need for security and confidentiality of both consumer and employee information.”
 - This language and other provisions of the Massachusetts regulation may sound familiar to those who are familiar with the banking agencies’ Interagency Guidelines and the SEC’s proposed information security revisions to Reg S-P
 - Security system requirements for computer and wireless networks on or through which personal information of Massachusetts residents is electronically stored or transmitted

- Required Elements in a Massachusetts WISP
 - The Massachusetts regulation prescribes several separately enumerated elements that must be included in a WISP, including the following:
 - Identification and assessment of reasonably foreseeable internal and external risks to the security, confidentiality or integrity of records containing personal information
 - Evaluation and improvement of the effectiveness of safeguards against information security risks, including employee training and compliance and means for detecting and preventing security system failures
 - Development of security policies for employees “relating to the storage, access and transportation of records containing personal information outside of business premises”
 - “Imposing disciplinary measures for violations of the comprehensive information security program rules”
 - “Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with” the regulation and applicable federal regulations

- Required Elements in a Massachusetts WISP (cont.)
 - “Requiring such third-party service providers by contract to implement and maintain such appropriate security measures for personal information” (subject to a phase in through March 1, 2012)
 - “Reasonable restrictions upon physical access to records containing personal information, and storage of such records and data in locked facilities, storage areas or containers”
 - Regular monitoring to ensure the WISP is “operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrading information safeguards as necessary to limit risks”
 - “Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information”
 - “Documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information”

- Massachusetts Computer System Security Requirements
 - The other main substantive part of the regulation – the requirement to establish and maintain a security system covering computers, including any wireless system – requires that the following elements, at a minimum and to the extent technically feasible, be part of the security system:
 - Secure user authentication protocols including
 - Control of user IDs and other identifiers
 - A reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies such as biometrics or token devices
 - Control of passwords to ensure that passwords are kept in a location or format that does not compromise the security of the data they protect
 - Restricting access to active users and accounts only
 - Blocking access after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system

- Massachusetts Computer System Security Requirements (cont.)
 - Secure access control measures that
 - Restrict access to those who need to know the information to perform their jobs
 - Assign unique identifications plus passwords – not vendor supplied default passwords – to each person with computer access that are reasonably designed to maintain the integrity of the security of the access controls
 - Encryption of all records and files containing personal information that are transmitted across public networks, and encryption of all data containing personal information to be transmitted wirelessly
 - Encryption of all personal information stored on laptops or other portable devices

- Massachusetts Computer System Security Requirements (cont.)
 - Reasonable monitoring of systems for unauthorized use of or access to personal information
 - For files containing personal information on a system connected to the Internet, reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information
 - Reasonably up-to-date versions of system security agent software that includes malware protection and reasonably up to date patches and virus definitions, or a version of such software that can still be supported with up to date patches and virus definitions and is set to receive the most current security updates on a regular basis
 - Education and training of employees on the proper use of the computer security system and the importance of personal information security

- Possible Penalties for Non-Compliance with the Massachusetts Information Security Regulation
 - The State Attorney General is charged with enforcing the law under which the regulation was promulgated
 - Under that law, violators could be subject to a \$5,000 civil penalty for each violation
 - How violations will be counted for purposes of the penalty is unclear
 - If violations are counted on a per-record basis, non-compliant businesses with thousands of records containing the personal information of Massachusetts residents could potentially face fines of millions of dollars

- What Does the Future Hold re State Information Security Laws and Regulations?
 - Several other states, including New Jersey, Michigan and Washington, have proposed or considered regulations or laws regarding the privacy and security of personal information of state residents
 - It is possible – and indeed seems likely – that, much in the same way the Massachusetts regulation drew from the banking agencies’ Interagency Guidelines and from the SEC’s proposed information security revisions to Reg S-P, other states may follow the federal and Massachusetts “lead” in adopting tough and specific information security laws and regulations that would apply to all businesses

- Information Security-Related Tips for Service Provider Contracts
 - Review Service Provider information security policy and practices in advance
 - Require Service Provider to represent, warrant and agree that it complies and will comply with applicable laws and regulations re information privacy and security, including reference to specific state laws (such as Massachusetts), if applicable
 - Require Service Provider to represent, warrant and agree that it will comply with Service Recipient's information privacy and security program, policies and procedures
 - Have Service Provider indemnify Service Recipient against breach or failure of any of the above, and consider carving the indemnity out from any liability limitation

- Questions about State Information Security Requirements?



MBA's NATIONAL TECHNOLOGY IN
MORTGAGE BANKING CONFERENCE & EXPO
APRIL 25-28, 2010, HYATT REGENCY CHICAGO

Federal Identity Theft Laws and Rules

Andrew Smith, Morrison & Foerster LLP

(202) 887-1558, asmith@mof.com

MORRISON

FOERSTER

Federal Identity Theft Laws and Rules

- Identity Theft and Assumption Deterrence Act (1998)
- FACT Act (2003)
- Identity theft = fraud committed or attempted using the identifying information of another person
- Primary Requirements:
 - » Identity Theft Red Flags Rule
 - » Address Discrepancy Rule
 - » Tradeline Blocking
 - » Fraud Alerts

Identity Theft Red Flags Rule

- Effective Dates
 - » Banks: Nov. 2008
 - » Non-banks (mortgage brokers, loan companies, non-bank servicers): June 2010
- Red Flag: indicator of possible existence of identity theft
- If you are a creditor or a depository institution
 - » You must determine whether you offer “covered accounts”
 - » “Covered Accounts” =
 - Consumer accounts involving multiple payments or transactions
 - Commercial loans, if a “reasonably foreseeable risk” to customers or safety & soundness from identity theft.

Identity Theft Red Flags Rule

- If you **offer** or **maintain** covered accounts, you must
 - » Develop and implement a **written** Identity Theft Program
 - Designed to prevent, detect, and mitigate ID theft
 - New accounts and existing accounts
 - » Be approved by the **Board** (or Board committee)
 - » Be overseen by senior management
 - » Include **staff training** and oversight of **service providers**
 - » Be **updated** to consider new threats as they arise
 - » Consider the **guidelines** provided by the agencies
- Guidelines
 - » **Identify** relevant red flags
 - » **Detect** those red flags
 - » **Respond** when red flags are detected
 - » **Administer** the ID Theft Program

- Risk assessment required
 - » Risk of ID theft to you or your customers
 - » New? Existing? Commercial?
- Key procedural requirements
 - » Must be in writing; must be approved by Board
- Much work may already be done
 - » AML/BSA, § 326 and CIP
 - » GLBA Safeguards
 - » FFIEC Authentication Guidance
- FTC and bank agencies
 - » Safety & soundness, guidelines, enforcement

Address Discrepancy Rule

- Credit bureau must notify user of credit reports when
 - » Address in user's request for credit report "substantially differs from" address in credit bureau file
 - » "Substantial difference" determined by credit bureau
 - » "Address discrepancy indicator" – different for each credit bureau: typically only a code in a specified field
- "Users" must respond to notice:
 - » All "users," not just lenders: depository institutions, landlords, insurers, employers
 - » All transactions, not just credit account opening, new card, or line increase
- You must develop and implement "reasonable procedures" to "form a reasonable belief" that credit report relates to the consumer
 - » Customer Identification Program (CIP) would satisfy requirement
 - » What happens when you cannot "form belief"?
 - Should not use credit report?
 - May trigger other requirements – like CIP and Red Flags Rule

Address Discrepancy Rule

- “Furnishers” also must respond to notice. If you:
 - » Can form a reasonable belief as to the consumer’s identity
 - » And “establish a continuing relationship” with the consumer – only new accounts, not existing accounts
 - » And regularly furnish information to the credit bureau that provided the address discrepancy notice
- Then you must have “reasonable procedures” for furnishing to the credit bureau an address for the consumer that you have “reasonably confirmed” is accurate.
- Examples of “reasonable confirmation”:
 - » Verifying address with consumer
 - » Verifying address using third-party data source
 - » Reviewing your own records to verify address

Tradelines Blocking

- Credit bureau must block reporting of ID theft-related tradeline
 - » Within 4 business days of receiving
 - appropriate proof of identity
 - ID theft report
 - identification of fraudulent information by consumer and
 - statement from consumer that consumer did not engage in transaction
 - » Must notify furnisher that information has been blocked
- Furnisher may not sell, transfer, place for collection debt subject to credit bureau block
 - » Exceptions:
 - repurchase from assignee
 - securitization of debt
 - pledging of portfolio as collateral
 - sale of the business

Tradeline Blocking

- Furnishers also may not “repollute” credit reports with ID theft-related trade lines
- Duty can be triggered by:
 - » Notice from credit bureau
 - Must have reasonable procedures to prevent furnishing
 - » Receipt of ID theft report from consumer
 - May not furnish unless you “subsequently know or are informed by the consumer” that info is correct
 - Key definition: “ID theft report”

Fraud Alerts

- Fraud Alerts
 - » Initial fraud alert
 - Upon request of consumer shall include a fraud alert in credit file and provide alert with any report or score generated for 90 days
 - Includes one free file disclosure
 - » Active duty alert
 - Stays in file for 12 months
 - Does not include a free file disclosure
 - » Extended fraud alert
 - Requires ID theft report
 - Stays in file for 7 years
 - Includes two free file disclosures within first 12 months.
- When “fraud alert” is in consumer report
 - » Initial Alert: lender must “form a reasonable belief” of identity of applicant before granting new credit, issuing additional card, or increasing line
 - Similar to USA PATRIOT Act
 - » Extended Alert: lender must contact consumer directly (e.g., by using phone number in alert)



MBA's NATIONAL TECHNOLOGY IN
MORTGAGE BANKING CONFERENCE & EXPO
APRIL 25-28, 2010, HYATT REGENCY CHICAGO

Recent Developments in Information Security Laws and Regulations

Developments At the Edge and Beyond

Henry L. Judy
henry.judy@klgates.com
202.778.9032

The logo for K&L GATES features the text "K&L" in a large, bold, black, sans-serif font, followed by a vertical red line, and then the word "GATES" in a similar bold, black, sans-serif font.

- Quon Case
- Social Media and Employer Liability
- High Tech Copiers

- City of Ontario, Calif. v. Quon
 - » Oral Argument before US Supreme Court on April 19, 2010
- Under the facts of the case
 - » Does government employee have a Fourth Amendment "reasonable expectation of privacy" in text messages transmitted on his pager?
 - » Was the City's the nature of review of the text messages reasonable?
 - » Do the senders of messages to the pager have their own reasonable expectation that the government entity would not review their messages?
- Ninth Circuit Held
 - » Yes
 - » No
 - » Yes

- Why important (in my opinion)
 - » Distinctions between rules applicable to government employees and private sector employees are becoming blurred, confused and subject to policy differences
 - » Misunderstandings of technology at the core of the case
 - » Expanded liability exposures
 - » Expansive policy arguments in play
 - » Important enough that the US Government (as Nation's largest employer) filed an amicus brief and appeared at oral argument on behalf of the city

- Facts

- » City had written policy warning employees not to expect privacy in their communications on city-owned computers and associated equipment. The policy, which was signed by Quon, allowed limited "light" personal use and reserved the right to monitor and log all network activity.
- » The policy: “[s]ome incidental and occasional personal use of the e-mail system is permitted if limited to ‘light’ personal communications[,]” which “may consist of personal greetings or personal meeting arrangements.”
- » Later Quon and other SWAT team members were given pagers. They were told orally by supervisors that the text messages were considered e-mail and were subject to the city's no privacy policy and possible audit.

- » Quon exceeded the character limit on his pager several times. A supervisor told him that he would not audit the overages to see if they were work-related but that Quon could pay for the overages, which Quon did.
- » While on duty, Quon used his pager to exchange hundreds of personal messages -- many sexually explicit -- with, among others, his wife, his girlfriend and a fellow SWAT sergeant.
- » Later after Quon and another officer had exceeded the character limit, the police chief ordered a review of their message transcripts to determine, the city contended, if the limit was too low. Review showed that on average only about 10% of Quon's transmissions during his shift were work related. He was reported for violating the department's policy on use of the pagers.

- » Quon, his wife, the girlfriend and his colleague sued the city, the police department and others alleging their Fourth Amendment rights were violated by the review of the text messages.
- » District court found that Quon had a reasonable expectation of privacy under a test announced by the Supreme Court in its 1987 decision, *O'Connor v. Ortega*, 480 U.S. 709, 717 (1987).
- » Under that test (plurality opinion), a government employee's expectation of privacy must be one "that society is prepared to consider reasonable" under the "operational realities of the workplace." (plurality opinion)..

- » Applying that standard, the court said Quon's expectation was reasonable because a supervisor had said he would not enforce the general computer policy.
- » Court submitted to a jury the question of whether the city's review of the messages was reasonable under the circumstances. The jury said yes, because the purpose was to determine the effectiveness of the character limit, not to ferret out misconduct.
- » Quon appealed the jury verdict on the reasonableness of the search. The 9th U.S. Circuit Court of Appeals reversed, finding that the scope of the search was unreasonable because it was excessively intrusive and that Quon and the other three plaintiffs all had a reasonable expectation of privacy in their messages

- **Arguments For the City**

- » 9th Circuit undercut "operational realities of the workplace" standard by allowing an employer's explicit, no-privacy policy to be abrogated by a lower-level supervisor's informal arrangement.
- » Enforceable "no-privacy policies are vital to public employers for maintaining the security and efficiency of electronic communications equipment.
- » California's public records law diminished Quon's privacy expectation because the public could get access to those text messages.
- » 9th Circuit's ruling "less intrusive methods" analysis that has been rejected by the justices and other circuits in the Fourth Amendment context.
- » The 9th Circuit erred in extending Fourth Amendment protection to the three other plaintiffs who exchanged text messages with Quon. Those three persons knowingly exchanged text messages with a government employee on a government-owned pager -- rather than on a privately owned pager -- could not reasonably expect that their messages would be free from review by the public employer.

- **Arguments For Quon**

- » City's computer policy was not revised to include the text-message pagers.
- » The only policy in effect was that of the low-level supervisor and he said he would not audit the text-messages as long as personnel paid for any overage charges
- » It was reasonable for Quon to assume anything he paid for personally was private. As Chief Justice John Roberts Jr. said at oral argument, "Now, most people will say, well, if you're paying for them, they are yours. And it particularly covered messages off-duty. Now, can't you sort of put all those together and say that it would be reasonable for him to assume that private messages were his business? They said he can do it. They said you have got to pay for it. He used it off-duty. They said they are not going to audit it."
- » The 9th Circuit is right in holding text messages are like to telephone calls and letters in finding a reasonable expectation of privacy
- » The city's interest in recovering the payment for the text messaging services could have been satisfied without allowing the search of the content of the messages.

- The most substantial issue in this case is the reasonableness of the level of review. The city's purpose was to determine whether the character allotment was appropriate. This enables the amici to argue that the Supreme Court should embrace the so-called "data minimization" principle which essentially would require that governments and other entities that collect and access individuals' personal information do so in a way that limits access and storage to the minimum amount of data necessary to accomplish a given task.
 - » This would be a very considerable expansion of US privacy law
- Under the 9th Circuit's holding, the review violated the 4th Amendment rights of the persons with whom Quon communicated privately. In a separate action Quon successfully sued Arch Wireless, the wireless pager provider, for having disclosed the messages to the city.
 - » Lesson: don't undertake a review until you consider the effects on third parties

- Seems clear that the policy as written did not explicitly cover text messages; equivalence of text messages and e-mail was communicated orally
 - » At oral argument issue was debated whether Quon should reasonably have concluded that they were equivalents
 - » **Lesson:** Be as specific as possible; don't create issues
- Most employers have boilerplate warnings of monitoring, but this boilerplate is meaningless if it doesn't accord with actual practices and if everybody understands it will be disregarded or not followed in certain contexts.
 - » **Lesson:** Don't allow situation (as in this case) where a lower level supervisor could be considered to have waived the policy.

- Consider a provision such as:
 - » While every effort has been made to have this Policy reflect the state of technology as of the date of its adoption [most recent revision], technological developments nonetheless may outstrip the literal text of certain aspects of this Policy. In view of the foregoing, the Company expects that users will be sensitive to the underlying spirit and intent of this Policy and will look to the goals this Policy is intended to achieve. They should not attempt to do indirectly what this Policy prohibits directly, and they should not employ means to defeat the goals that this policy is intended to achieve, even though these means may not have been mentioned in this Policy.

- **Selected References**

- » SCOTUS Wiki on case:
http://www.scotuswiki.com/index.php?title=City_of_Ontario_v._Quon
- » Opinion of the United States Court of Appeals for the Ninth Circuit is reported at 529 F.3d 892 (9th Cir. 2008).
- » Ninth Circuit's order denying rehearing and rehearing en banc, including a one-judge concurring opinion and a seven judge dissenting opinion, is reported at 554 F.3d 769 (9th Cir. 2009)
- » The opinion of the United States District Court for the Central District of California is reported at 445 F. Supp. 2d 1116 (C.D. Cal. 2006)
- » Amicus Brief of the United States
http://www.abanet.org/publiced/preview/briefs/pdfs/09-10/08-1332_ReversalAmCuUSA.pdf
- » Amicus brief of Electronic Privacy Information Center (EPIC) et al. http://epic.org/privacy/quon/Quon_Brief_Draft_final.pdf

- » Amicus brief Electronic Frontier Foundation, et al.
http://www.aclu.org/files/assets/08-1332_bsac_Electronic_Frontier_Foundation_et_al.pdf
- » Important recent New Jersey Case: Stengart v. Loving Care Agency, Inc. <http://lawlibrary.rutgers.edu/courts/supreme/a-16-09.opn.html> (Private employer; employee used company laptop to communicate with personal lawyer; employee has expectation of privacy; search was unreasonable)
- » American Management Association, The Latest on Workplace Monitoring and Surveillance, Mar. 13, 2008, <http://tinyurl.com/yjb4q4a>

- Oceans of digital and physical ink have been spilled on subject of social media. I want to focus strictly on the essentials of when an organization can be held responsible for the social media actions of its employees
- Not cover:
 - » Corporate blogs
 - » Employees (often marketing department employees) whose job it is to contribute to social media platforms on behalf of employers
- Consider on two levels
 - » General law
 - » Specific regulatory controls
- On the general law level, nearly everything can be summed up under the heading of the common law rule of “respondeat superior” (Latin: “let the master answer” – that is, be liable, answer in damages) The idea is that normally an employer is responsible for the actions of its employees performed within the course of their employment.

- If the employee's acts are not within the course of their employment, the employee is said to be “off on a frolic and detour” of his/her own and the employer is not liable
 - » For example, volunteer “astro-turfing” by employee - artificial creation of a grassroots buzz for a product, service or political viewpoint
- The determination if whether the employee is or is not acting in the course of his employment is highly fact-specific and can depend on a number of factors, but the principal issues are:
 - » What instructions the employee was given
 - » Whether the employee can reasonably be considered to have understood them
- In short, what does the Company policy say and was it clearly communicated?

- On the level of specific regulatory controls
 - » False advertising under the FTC Act and equivalent state laws
 - In particular, the recently revised FTC Guidelines: see, “Guides Concerning the Use of Endorsements and Testimonials in Advertising,” 16 C.F.R. Part 255. See <http://www.ftc.gov/opa/2009/10/endortest.shtm>. In brief, bloggers who make an endorsement must disclose the material connections they share with the seller of the product or service.
 - On January 25, 2010, the Financial Industry Regulatory Authority (“FINRA”) issued Regulatory Notice 10-06, Guidance on Blogs and Social Networking Web Sites for securities firms, investment advisors and brokers. The Guidance includes requirements that covered firms should (i) retain records of communications made through social media sites; (ii) consider adopting policies and procedures governing communications that promote specific investment products; (iii) supervise electronic communications in a manner “reasonably designed” to ensure that they do not violate FINRA rules; (iv) prohibit employees from engaging in business communications on social media web sites that are not subject to the firm’s supervision; and (v) screen third-party content on firm-sponsored blogs or social networking web sites. <http://www.finra.org/Industry/Regulation/Notices/2010/P120760>
- I’d like to step through a comprehensive and restrictive policy and show why the various element are in it and how varying it changes the results.

- Use of Web 2.0 technologies refers to the creation of user-generated content using certain Internet-based technologies such as blogs, vlogs, wikis, social networks, podcasts, virtual reality worlds and the like. This policy deals with use of Web 2.0 platforms sponsored by third-parties; it does not deal with any such platform sponsored by the Company itself.
- Web 2.0 technologies are developing at a rapid pace and this policy is intended to cover Internet-based technologies not specifically mentioned above and future Internet-based technologies having the same function and effect.
 - » This helps avoid the argument that “I didn’t understand that Twitter is a Web 2.0 technology.”
- Use of the Company’s Information Processing Facilities to access Internet-based external e-mail accounts (Yahoo!, Google, MSN, etc.), and non-professionally related message boards / chat rooms, blogs, wikis, social networking sites or other Web 2.0 platforms is prohibited.

- » Unless you are a member of the Company's marketing staff, in which case there should be a separate set of guidance
- Whether or not a Company employee chooses to create or participate in some form of online publishing or discussion using Web 2.0 technologies is his or her own decision. However, such choices are subject to certain limitations insofar as they affect the Company
 - » The use of Web 2.0 technologies by Company employees is for individual interactions, not for Company communications. When the Company wishes to communicate publicly as a firm, it will do so by officially authorized means and spokespersons.
 - » Never use these technologies to refer, however indirectly, to any customer, customer matter, potential customer matter or competitor of the Company
 - Otherwise, risk of defamation
 - » Never refer to another Company employee, vendor partner or supplier without clear prior permission. Respect the privacy of your co-workers.

- If your post raises concerns, don't drag others onto it
- » Do not provide the Company's or another's confidential or other proprietary information. In particular, do not include the Company's logos, trademarks, or other intellectual property in your postings.
 - Otherwise, there is a risk of security law violations, loss of trade secret protection, violations of confidentiality agreements, etc
- » Do not use the logos, trademarks, or other intellectual property of third parties in your postings without the explicit permission of the third parties
 - Helps avoid claims of direct and contributory Lanham Act violations
- » Respect copyright, fair use and financial disclosure laws.
- » If you refer to any other matter related to the Company, identify yourself and write in the first person. You must make it clear that you are speaking for yourself and not on behalf of the Company
 - Note that this paragraph does not prohibit anonymous postings or pseudonymous (using a handle or screen name) postings generally; only such postings if on a matter related to the Company

- » If you refer to yourself as an employee of the Company, you must include a disclaimer to the effect that “These postings are my own and don’t necessarily represent the views of Company”.
- » When in doubt whether a matter is appropriate for sharing or discussion using Web 2.0 technologies, consult with appropriate other staff of the Company and, in the meantime, be silent.
- » Your use of Web 2.0 technologies must be consistent with other applicable Firm policies, including this Policy on Use of Company Information Processing Facilities.
- » Anyone participating in a social network for any reason is responsible for reading, understanding, and complying with the site's terms of use
- » Due to confidentiality and privacy concerns, users are prohibited from importing or uploading any customer contacts to any networking sites.
 - Customer contacts belong in the Company’s CRM application. At best you are giving a way valuable commercial information. This is a particular concern for global companies since it is likely to violate the EU Data Protection Directive

- » Refrain from taking any position on any issue involving the Company that is pending before the courts, in arbitration or before any governmental body
- » Obtain approval from the Company's General Counsel function before responding to inaccurate, accusatory, or negative comments about the Company, its employees, or its customers, inquiries from journalists on issues related to the Company, its employees, or its customers
 - A Company issue is never advanced by private flame wars
 - Always let the pros handle conversations with journalists; otherwise you are juggling with knives
- » In the end, employees are personally responsible for their posts. The Company will accept no responsibility for your postings

- Modern, large, office-type photocopiers are computers. The whole system is controlled by a computer which has a hard disk. The copier scans images and they, with all personal and sensitive data, are stored on the disk.
- These copiers are also networked computers, and they have all the same security issues that a computer does
- THEY ARE ALSO A GOLD MINE FOR THEIVES OF PERSONAL AND OTHER SENSITIVE DATA
- Typical exposures
 - » Photocopiers are picked up when the lease is almost over and if in good shape are auctioned off to middlemen and resold.
 - » Some end up with dealers
 - » Some are sold through Craigslist or similar sites
 - » Many are likely still have crucial data on them.
 - » Some dealers remove the hard drives and purge them before they are picked up for resale or they replace the hard drives. But that costs extra time and money

- This does not apply to all copier/scanning equipment. For example, Xerox has a feature called Image Overwrite that automatically overwrites the data after every use
- You choices are:
 - » Wipe the disks as you would any other storage device upon disposal
 - » Hire a specialist wiping firm
 - » Trust your vendor
 - » Combination of the foregoing
- In any case:
 - » Add this risk to your protocols
 - » If relying third party get a certificate of proper disposal
- For detailed info see Digital Copier Security, Inc
(<http://www.copiersecurity.com/>) – not an endorsement

- Recently a CBS News investigation found that sensitive police department information was on the hard drives of two copy machines the city of Buffalo had leased from Toshiba. The machines were sold in New Jersey. <http://www.buffalonews.com/2010/04/22/1027554/city-fires-attorney-who-handled.html>
- On April 5, 2020 Affinity Health Plan announced that an office copier it had previously leased and since returned to the leasing company may contain personal information on its hard drive. See https://www.affinityplan.org/uploadedFiles/Affinity_Home/Who_We_Are/PressRelease_040510.pdf. In its notification to the NYS Consumer Protection Board about the breach, the company indicated that 409,262 NY State residents were affected. a report by CBS News on April 15 confirms that some 300 pages of individual medical records were on the hard drive. See <http://www.phiprivacy.net/?s=copier&x=12&y=5>

- This is an issue at the edge. European data protection supervisor Peter Hustinx recently called for data-wiping technology to be built in to electric and electronic equipment. He did so in the course of a review of the European Commission's proposed revision of the Waste Electrical and Electronic Equipment (WEEE) directive. He also wants WEEE to ban the sale of used electronic devices that have not been wiped clean of data.
 - » See opinion at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-04-14_Opinion_WEEE_EN.pdf
- Our prescient moderator Bruce Nielson called attention to this issue over three years ago in an speech to the records management association, ARMA International.

