Privacy on the Internet

HP World 2002 – Session 568

Ben Rothke, CISSP
Senior Security Architect
QinetiQ Trusted Information Management

brothke@QinetiQ-tim.com

About me...

- Senior Security Architect with QinetiQ Trusted Information Management
- Previously with Camelot Information Technologies, Baltimore Technologies, Ernst & Young, Citibank
- Have worked in the information technology sector since 1988 and information security since 1994
- Frequent writer and speaker
  - Unix Review
  - Security Management magazine

About QinetiQ Trusted Information Management

- Premier team of the world’s leading Information Protection and Operations experts
- Division of QinetiQ’s Knowledge and Information Systems organization
- 9,000 staff worldwide
- 220 QTIM staff in UK and US
- Internationally-renowned authors, architects, practitioners and consultants

Session agenda

Topics to be discussed:

- Defining privacy
- Protecting Privacy
- Privacy Solutions
- Privacy Regulations
- What to Do
- Resources
- Q&A

This session is not:

- In-depth analysis of privacy
- Legal, privacy or social issues

Please feel free at any point today to make a correction, share a story, make a comment, etc.

This session isn't meant to be a monologue!! ☺

What is Privacy?

What is Privacy?

Privacy is an abstract and often elusive term that is often difficult to effectively define.

- The ability of an individual or organization to decide whether, when, and to whom personal or organizational information is released.
- Informational self-determination
- The right to be left-alone
- Even *whatis.com* can't give a good definition of privacy

What is Privacy?

From Dictionary.com:

pri•va•cy - noun

1. a. The quality or condition of being secluded from the presence or view of others.

   b. The state of being free from unsanctioned intrusion: a person's right to privacy.

2. The state of being concealed; secrecy.

What is Privacy?

Privacy means radically different things to different people.

- Prosser's four categories of invasion of privacy from a tort perspective are:

  1. Intrusion – the unreasonable and highly offensive intrusion upon someone's solitude.
  2. Appropriation – the unauthorized use of someone's name, likeness or other information related to identity.
  3. False light – the highly offensive, false portrayal of an individual.
  4. Disclosure of private facts – the highly offensive publication or distribution of private information that is not of legitimate public interest.

- Since the publication of Prosser's paper in 1960, these four torts have, in general, been recognized as the only grounds for legal action based on invasion of privacy.

Is privacy in the Internet era fruitless?

- Scott McNealy
  - *"You have zero privacy anyway. Get over it!"*
- Zero Knowledge Systems
  - The ZKS Freedom Network was built from the ground-up for privacy by extremely bright and security savvy designers.
  - It was shutdown in October 2001 due to lack of public interest. The reason: Few people were willing to pay extra to cloak their identities while browsing the web or sending e-mail.
- PGP (Pretty Good Privacy) software
  - provides superb e-mail and file level encryption
  - PGP was sold off by NAI in October 2001 due to lack of profits.
  - "There wasn't a lot of market demand around for what we were doing"
    - Michael Callahan, marketing director at McAfee

Protecting Privacy

Privacy starts with the individual

The most effective privacy tool is a person's desire for it!

- How important is privacy to you? If you *really* desire privacy, move to a cave, pay cash for everything and stop:

- filling out web surveys
- applying for free credit reports
- using credit cards
- using prescription medication
- flying via commercial airlines
- subscriptions to magazines
- buying via mail order
- sending in warranty cards
- registering software
- having children in hospitals
- getting reimbursed for health insurance medical visits
- using frequent flyer and other type of reward programs
- using customer cards at grocery and retail stores
- using toll collection systems
- checking out books from the library & renting videos

Effective privacy requires being proactive

- Once your personal information or client data has been leaked beyond limits, it's too late to do anything – as the spread of the information can't be undone.

- Esther Dyson - "I've also been disappointed in consumers in that they've not been proactive in protecting their own data. You do a survey and consumers say they are very concerned about their privacy. Then you offer them a discount on a book and they'll tell you everything."

Privacy and controlling data access

If organizations truly want to protect their user's and client's privacy, and not suffer negative PR from violation issues, every aspect of the privacy and information security infrastructure must be managed, as privacy can't be protected in a vacuum.

- Policies and procedures
  - For day-to-day business issues and to minimize litigation
- Acceptable use
- Expectations of privacy
- Physical security
- Access control
- Database security
- Encryption
- Incident response

Privacy & controlling data access

- Few people really know what is happening on their networks and systems.
- Most people designing, implementing and operating these networks and systems work in their own area of expertise, knowing a lot about their piece of the puzzle, but not about why they should or how they should work together.
- Lack of good and proficient training
  - Why do we have books such as *Learn to Write Flashy Web Sites in 24 Hours,* but not books such as *Learn to Fly a Learjet in 24 Hours?*
- Most companies don't take information security and privacy seriously
  - How many people were fired for sharing their password?

Threats to privacy

- Compilation and Centralization
  - 25 TB databases are not state of the art anymore
- Linkability
  - HTTP Cookies, SSN, user names
- Data mining
  - Have my data talk to your data
- Leaky channels
  - Chatty protocols (HTTP & HTML)
- People
  - Those taking an Internet poll said privacy is critical
  - And then proceeded to give the web site huge amounts of personal information in order to get the results of the poll
- Rapid pace of technological change

Privacy Solutions

Encryption

- While encryption is the foundation for security and privacy, it has been shown that the average end-user simply can’t be expected to correctly configure and use encryption software.
  - See *Why Johnny Can’t Encrypt: A Usability Evaluation of PGP*
- We are at least a decade away from having seamless encryption functionality built into software and hardware products. Even then:
  - people will use ineffective passwords
  - software companies will use proprietary cryptographic algorithms in their products
  - physical security will be ignored

Cookies

Cookies themselves are not a threat to privacy.

- A cookie is information that a web site puts on a users' drive so that it can remember something about the user at a later time.
- The very nature of web servers allows for the tracking of a user's surfing habits. Other individualized information about the user can be gathered with time.
- While cookies themselves are not gathering that data, they are used as a tracking device to assist the people who are gathering that information. As information is gathered about the user, it is associated with the value that is kept in the cookie.
- While privacy advocates scream at cookies, they forget about log files. Compared to log files, cookies only provide a tiny piece of added tracking ability.

Son of Cookies?

- Cookies can be easily deleted or disabled, and can only return to a web-server information downloaded by the same web-server on a previous visit. So their use as information gathering devices is limited and provides only crude and inaccurate representations of web activity.
- A new, sensor based cookie-like architecture means that it:
  - can be individually customized for any web visitor
  - can collect information rather than return pre-downloaded data.
  - can be reconfigured remotely
  - is difficult to detect and delete
  - can be used to block access to sites, documents, data, monitor keystrokes, e-mails, etc., based on content,
  - can be preferentially customized for each user
  - See www.eee.strath.ac.uk/news/internet-monitor.htm

Filtering

- While filters can be effective to a degree, we have to realize that even when things are filtered, they will eventually fill up.
  - Filtered cigarettes don’t prevent cancer, they only delay it.
- With a reasonable amount of time and resources, the efficacy that filters afford are minimal.

Privacy seals for web sites

- The function of a privacy seal is to reassure web site visitors about their privacy.
  - Visitors to the web site can find out what the site will do with personal data obtained and how they will disclose it.
- Privacy seals seem to primarily benefit the (for profit) company's selling the seals.
- Many privacy seals afford a level of privacy acceptable to Prosser (tort), but not according to the expectation of privacy that many consumer expect.
  - You must read the fine print and disclaimers when clicking on the privacy seal.
  - Will the privacy vendor revoke the seal if the web-site breaches its privacy polices? In many instances, they have not.

Privacy seals

- TRUSTe
- Gold Privacy Seal
- AICPA WebTrust
- PwC BetterWeb
- BBBOnLine Reliability seal
- E&Y CyberProcess Certification

How trusty is TRUSTe?

- Yahoo has had the TRUSTe seal for a number of years
- In early 2002, Yahoo announced sweeping changes in the way it uses customer data collected under previous privacy policies. Does this make the Truste seal meaningless? Some say yes.
- TRUSTe doesn't attempt to set privacy policies. It only ensures that companies clearly state their own rules for handling customer data & then adhere to them.
  - It can make suggestions & demand documentation of compliance with contracts, but can't send auditors onsite to review systems and records, nor does it have any direct enforcement authority.
- Esther Dyson – "TRUSTe's image has slipped from consumer advocate to corporate apologist. The board ended up being a little too corporate, and didn't have any moral courage".

TRUSTe debacles in the news

- Choicepoint
  - left an internal corporate database viewable to anyone with a browser
- DoubleClick
  - Hacker loaded a back-door program on the company's Web server and had viewed files on another server hosting its Abacus Online database
- RealNetworks
  - Surreptitiously gathered data about the music listening habits of its users and recorded that information
- Toysmart.com
  - assured its customers that their personal information would never be shared with a third party, but decided to sell their customer database after going out of business in May 2001.
  - But TRUSTe fought against their client on this one!

Privacy Regulations

Prominent U.S. Privacy Laws

- GLBA - Gramm-Leach-Bliley Financial Services Modernization Act
- HIPAA: Health Insurance Portability and Accountability Act
- 21 CFR Part 11: FDA Electronic Records & Electronic Signatures
  - Applies to all FDA regulated program areas and establishes technical and procedural standards regarding electronic record keeping and electronic signatures.
- COPPA: Children's Online Privacy Protection Act
  - Applies to the online collection of personal information from children under 13. The rules spell out what a web site operator must include in a privacy policy, when and how to seek verifiable consent from a parent and what responsibilities an operator has to protect children's privacy and safety online.
- CIPA: Children’s Internet Protection Act
  - Safety policies address minors access to *inappropriate matter*
- Fair Credit Reporting Act of 1999
  - Responsibilities under the law to parties who obtain consumer reports from the agency.

Additional U.S. Privacy Laws

- CCRRA - Consumer Credit Reporting Reform Act of 1996
- FTCA - Federal Trade Commission Act
- ECPA - Electronic Communications Privacy Act of 1986
- CCPA - Cable Communications Policy Act of 1984
- RFPA - Right to Financial Privacy Act of 1978
- EFTA - Electronic Funds Transfer Act
- VPPA - Video Privacy Protection Act
- DPPA - Drivers Privacy Protection Act of 1994
- TCPA - Telephone Consumer Protection Act of 1991
- ADA - Americans with Disabilities Act
- Privacy Act of 1974
- Patriot Act of 2001
- more to come………

State privacy laws

State Laws

- Currently, 12 states recognize right to privacy
- California is only one protect against both government & private intrusions
- New CA law - SB168 – October 11, 2001 - Bans the public posting of individual social security numbers
  - prohibits persons and entities from requiring SSN to access products or services
  - requires secure connections or encrypted use of SSN for Internet transmission
  - prohibits the printing of SSN on mailed materials (unless required by state or federal law)
  - does *not* prevent the use of SSN by persons or entities for internal verification or administrative purposes

International privacy laws

- European Union Data Protection Directive of 1995
  - Contains 33 articles in 8 chapters.
  - Effective October 1998
- Six areas:
  - **Notice** - An individual has the right to know that the collection of personal data will exist.
  - **Choice** - An individual has the right to choose not to have the personal data collected.
  - **Use** - An individual has the right to know how personal data will be used and to restrict its use.
  - **Security** - An individual has the right to know the extent to which the personal data will be protected.
  - **Correction** - An individual has the right to challenge the accuracy of the data and to provide corrected information.
  - **Enforcement** - An individual has the right to seek legal relief through appropriate channels to protect privacy rights.

International privacy laws

Safe Harbor

- As of mid-2002, 186 organizations participating
- A framework created by the U.S. Department of Commerce approved in 2001 by the European Commission
- Provides a privacy compliance framework for US organizations regulated by the FTC or DoT to avoid experiencing interruptions in their business dealings with the EU or facing prosecution by the European authorities under European privacy laws
- Certifying a US organization to the Safe Harbor requirements will assure that EU entities know that the organization provides adequate privacy protection as required by the EU Directive

Privacy Regulations

HIPAA & GLBA

What is HIPAA?

- **Health Insurance Portability & Accountability Act**
  - Essentially insurance reform
  - Presented to Congress as the Kassenbaum-Kennedy Bill
  - Public Law 104-191 - signed into law in August 1996.
  - HIPAA has its roots in the 1993 Clinton healthcare reform proposals. Its primary intent is to provide better access to health insurance, limit fraud and abuse & reduce administrative costs.
  - Also meant to ensure that individuals between jobs have the ability to continue their previous insurance coverage or obtain similar coverage
  - Protection of transmitted information

What is HIPAA?

- Addresses
  - Standardization of formats and codes
  - Security of all electronic patient data
  - Patient privacy
- Improve the efficiency & effectiveness of the healthcare organization systems by standardizing the interchange of electronic data for specified administrative and financial transactions
- 25% of HIPAA is technology and 75% is policies and procedures.
  - Similar to a diet, which is 25% food & 75% exercise and will-power.

HIPAA privacy will transform healthcare

- HIPAA will change nearly every business process within a healthcare organization. It will affect how:
  - Information is processed and exchanged
  - Claims are submitted and remittance received
  - Referrals are certified and authorized
  - Benefits are coordinated
  - Providers, health plans, and patients are identified
  - Data is protected
  - Individual privacy is preserved

- These changes don't come cheap as the expenditures for HIPAA will be huge.

Administrative Simplification

- HIPAA’s portability (given the increased risks imposed by the move to electronic transactions) requires the secure transfer of medical information.
  - Anticipating this, a separate section of provisions, independent from the insurance reform provisions was added under Subtitle F, Part C - *Administrative Simplification*.
- Administrative Simplification necessitates creation of standards and requirements for the maintenance and transmission of health information that identifies individual patients.
- The security & privacy provisions of HIPAA are the most challenging federal information technology requirements facing Covered Entities today.

HIPAA is built on common sense security

A lot of security problems can be obviated by following common sense practices:

- Have a trained information security staff
- Design a common information systems security architecture
- Don’t speak about patient issues in public places (elevator, cafeteria, lobby, cell phone etc.)
- Secure your database servers in protected physical environment
    - The security architecture of all network operating systems (Windows NT, NetWare, Solaris) are all built on a secure physical infrastructure
- Make sure the party you are communicating with is legitimate and authorized (Social Engineering)
- Develop a comprehensive set of information system security policies
- Correct SANS Top 20 most critical internet security vulnerabilities
    - www.sans.org/top20.htm

Penalties

An individual who knowingly & in violation of HIPAA obtains or discloses individually identifiable health information can be penalized.

Wrongful Disclosure

- *For each offense;*
- Fined not more than $50,000
- Imprisoned not more than 1 year

False Pretenses

- Fined not more than $100,000
- Imprisoned not more than 5 years

Intent to Sell, Transfer, or Use

- Fined not more than $250,000
- Imprisoned not more than 10 years

Non-criminal penalties

- HIPAA violations can turn into a PR nightmare.
  - Significant financial penalties
  - Bad press
  - Potential loss of JCAHO/NCQA accreditation
  - Unfavorable Legislative Audits
- Third-party reviews (Joint, US News & World Report, consumer magazine, etc.) will take HIPAA compliance into consideration.
- Non-compliance or failure will directly affect bottom line.

Gramm-Leach-Bliley Act

- GLBA mandates (effective July 1, 2001) that financial service businesses provide customers with a clear and conspicuous initial and& annual notice of their privacy policies.
- If non-public personal information is shared with non-affiliated third parties, the ability to opt-out of such sharing.
- GLBA affects a quarter of a million financial service businesses
  - banks
  - thrifts and credit unions
  - consumer finance companies
  - mortgage lenders & mortgage brokers
  - insurance agents
  - real estate agents
  - stockbrokers and financial planners

Gramm-Leach-Bliley Act

- GLBA security provisions require the FTC & certain other federal agencies to establish standards for financial institutions relating to administrative, technical & physical safeguards for customer data.
- The federal bank regulatory agencies have already issued their standards. As is the case with the federal bank regulatory standards, objectives of the FTC's standards are to:
  - ensure the security and confidentiality of customer records and information
  - protect against any anticipated threats or hazards to the security or integrity of such records
  - protect against unauthorized access to, or use of, such records or information that could result in substantial harm or inconvenience.

Gramm-Leach-Bliley Act

- More than a billion GLBA notices have been mailed, often requiring a law degree to penetrate the *wherefores* and *therefores*.
- However carefully or poorly worded the statements may be, the onus is ultimately on the consumer to tell the companies they do business with not to sell their personal data.
- GLBA in a nutshell:
  - *We reserve the right to sell and/or share information we have about you to telemarketers, credit card companies, spammers and others unless you tell us not to.*
- Before GLBA was signed, a bill was authored for stronger laws that would prohibit the sale of personal data unless a consumer specifically *opted in*. But lobbyists for the banks, mortgage firms & credit card companies prevailed. Now the burden is on the consumer.

Gramm-Leach-Bliley Act

GLBA Impact

- An individual can be fined up to $250,000 and/or 5 years prison per incident if no other U.S. laws were also broken.
- An individual can be fined up to $250,000 and/or 10 years prison per incident if other U.S. laws were also broken.
- An organization can be fined up to $500,000 per incident and/or the primary organization defendant(s) imprisoned for 5 years per incident if no other U.S. laws were also broken.
- An organization can be fined up to $500,000 per incident and/or the primary organization defendant(s) imprisoned for 10 years per incident if other U.S. laws were also broken.

What to do

Chief Privacy Officer

- Hottest New Job Title
  - Chief Chief Privacy Officer
- Has Legal Experience/Knowledge and understands the limits and risks of information technology
- Brings staff together with new solutions
- Educates and reassures workers, customers, prospects, investors and the public
- Develops Principles, Policies, & Procedures
- Serves As Dispute Resolution Ombudsman
- Obtains Seals Of Approval From Third Parties

Privacy Policies

- Surveys indicate posted policies increase customer confidence and trust and encourage personal disclosure of information at the site
- Protect organizations by explicitly defining commerce boundaries and customer relationships
- Establish a personal information sharing process for ALL web site visitors, removing the need to address issues with each individual

Privacy Policies

- Policies need to inform web site visitors of the organization’s information handling procedures
- Good privacy policies demonstrate compliance with laws, regulations, social customs and due diligence
- Policies illustrate your organization’s ethical values and genuine concern for customer welfare
- Posting policies is a requirement of many 3rd-party organizations
- Policies establishes rules when laws are lacking
- Base policies on your business environment, industry, and applicable legal requirements

Customer Privacy Policies

Keep these pointers in mind:

- Keep it simple
- Make it easy to find on the Web site
- Make it easy to read and understand
- Summarize it concisely and accurately in an easy-to-understand leading statement
- Communicate and promote it internally in employee communications and training sessions!!
  - You must ensure everyone understands the policy and follows it, or it will fail, and could put your organization in legal jeopardy
- Promote it with key stakeholders, including customers, investors, vendors, contributors and policymakers
- Update to stay current with changes in your business and the law

Samples Customer Privacy Policies

- No information will be gathered without the customer’s knowledge
- Customers may request their records for review and may challenge errors in their records and request the organization to investigate
- Customers may add comments within their records to indicate their opinion or situation of their reported errors that are not corrected to their satisfaction.
- Customers may determine whether or not they receive advertising and other marketing-related information
- Your organization wont sell customer information to third parties without the express permission of the customer, or as a legal requirement.
- Customer information is encrypted while it passes through the Internet
- Explanation of how your organization uses cookies and web server logs
- Explanation of why your organization collects the information it does at the web site

Avoiding Privacy Violations

- Often accidental in nature
- A privacy violation may result from:
  - User’s own disclosure
  - Third party intelligence
  - Misconduct
  - Accidental leak
  - Failure or insufficient notification of changes

Fair Information Practice Principles

1. Notice/Awareness
2. Choice/Consent
3. Access/Participation
4. Integrity/Security
5. Enforcement/Redress

Secure servers

- Any server that stores private data must be appropriately secured
  - Harden operating system
  - encrypt data
  - use router ACL to restrict access to data servers
  - remove unneeded accounts, services and protocols
  - patch operating system and applications
  - ensure software applications are written securely
  - code reviews
  - train administrators

Resources

Web sites

- www.privacyinternational.org
- www.privacyexchange.org
- www.privacyrights.org
- www.privacytimes.com
- www.privacy.org
- www.ftc.gov/privacy/index.html
- www.pandab.org
- www.privacyorganization.org
- www.privacyalliance.org
- www.PrivacyDigest.com
- www.privacyfoundation.org

Recommended Reading

- Web Security, Privacy and Commerce - Simson Garfinkel
- Database Nation - Simson Garfinkel
- World Without Secrets: Business, Crime and Privacy in the Age of Ubiquitous Computing - Richard Hunter
- ISP Liability Survival Guide: Strategies for Managing Copyright, Spam, Cache, and Privacy Regulations - Timothy Casey
- Developing Trust: Online Privacy and Security - Matt Curtin
- The Electronic Privacy Papers: Documents on the Battle for Privacy in the Age of Surveillance - Bruce Schneier
- Privacy Defended: Protecting Yourself Online - Gary Bahadur
- HIPAA Handbook: What Your Organization Should Know About the Federal Privacy Standards - Alexander Brittin

Conclusions & Recommendations

Conclusions

- The sheer power of distributed computing and shared resources makes the preservation of personal privacy extremely difficult.
- Privacy is like weight loss, you really have to want it and you must constantly work at it.
  - Even with all of the diet drinks and fat-free foods, people are not getting any thinner.

Conclusions

- Unfortunately, privacy issues will continue to get much worse before it gets better.
- Don’t rely on Federal laws to protect your privacy.
  - It is debatable if there will *ever* be Federal privacy protection
- Individual state privacy laws, where they exist are inconsistent.
- Bottom line - **Companies must take security and privacy seriously and follow-though with effective policies and procedures to protect the data privacy of their user’s and client’s.**

Thanks for attending

- Any questions? comments?
- Thanks for attending!

Ben Rothke, CISSP
Senior Security Architect
QinetiQ Trusted Information Management
Office 973/591-0129
Mobile 973/489-0838
brothke@QinetiQ-tim.com

www.QinetiQ-TIM.com
www.QinetiQ.com