



Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

May 04, 2011



ISOAG May 2011 Agenda

- | | | |
|------|---|---|
| I. | Welcome & Opening Remarks | John Green, VITA |
| II. | Privacy: How Did We Get Here? | Ed Miller, DOA |
| III. | Personnel Security:
A Short Review of SEC 501-01 | Bob Baskette, VITA |
| IV. | Upcoming Events & Other Business | John Green, VITA |
| V. | Partnership Update | Bob Baskette, VITA
Michael Clark, NG |

Privacy: How did we get here?

Timeline of how
technology affects privacy

Ed Miller
Department of Accounts



1776

1835

1890

1950

2017

Privacy: definition

The “legal” definition for privacy, typically cited in court cases is:

“the right to be left alone”

Warren & Brandeis in the 1890
Harvard Law Review.

However, to provide services, government can't leave you alone. We need personal information to do it.

- Birth records
- Driver's license
- Marriage license
- Divorce decree
- Tax returns
- Permits & licenses
- Grades & diplomas
- Traffic tickets, court orders
- Death certificates
- And much, much more.

How do we balance what government needs and what technology can do with an individual's privacy or their "right be left alone"?



PRIVACY encompasses the rights and obligations of individuals and organizations with respect to the...

- ***Collection***
- ***Use***
- ***Disclosure, and***
- ***Retention***

...of “***PERSONAL INFORMATION***”.

So what is “***PERSONAL INFORMATION***”?

§ 18.2-186.6 (Virginia breach of personal information notification)

"Personal information" means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted:

- ❑ Social security number;**
- ❑ Driver's license number or state identification card number issued in lieu of a driver's license number; or**
- ❑ Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts.**

■ **§ 2.2-3801 (Virginia Government Data Collection and Dissemination Practices Act)**

"Personal information" means all information that:

(i) describes, locates or indexes anything about an individual including, but not limited to:

social security number, driver's license number, agency-issued identification number, student identification number, real or personal property holdings derived from tax returns, and his education, financial transactions, medical history, ancestry, religion, political ideology, criminal or employment record, or

(ii) affords a basis for inferring personal characteristics, such as:

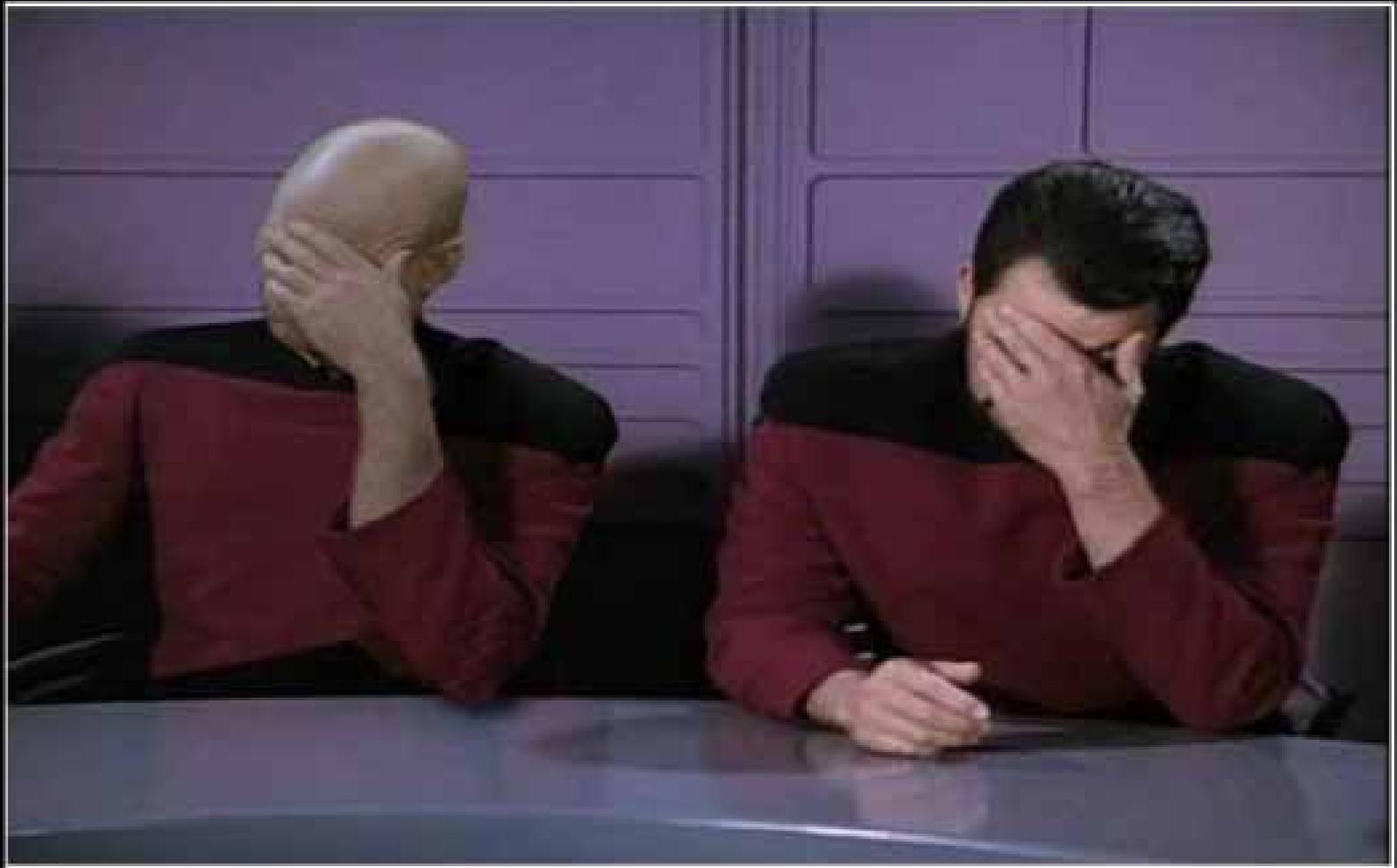
finger and voice prints, photographs, or things done by or to such individual; and the record of his presence, registration, or membership in an organization or activity, or admission to an institution.

Personal Information per HIPAA

1. Names
2. Geographic subdivisions smaller than a state (including zip)
3. All elements of birthdate except year
4. Telephone numbers
5. FAX numbers
6. Email address
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate or License numbers
12. Vehicle identifiers: license plates, device identifiers & serial #'s
13. URL's
14. IP addresses
15. Biometric identifiers
16. Full face photos and comparable images
17. Any unique identifying number, characteristic or code.

State Data Breach Notification Laws

- 46 states now have a data breach notification law.
- Many states have followed the example of California's SB 1386 (2003) notification law.
- California requires any agency, person or business that owns or licenses computerized 'personal information' to disclose any breach of security to **any California resident** whose unencrypted data is believed to have been disclosed.
- The statute applies regardless of whether the computerized personal records are maintained in or **outside California.**



DOUBLE FACEPALM

When the Fail is so strong, one Facepalm is not enough.

Epsilon

- Some people are calling the hack of email mass marketer Epsilon the largest data breach ever.
- For the most part, it appears only names and email addresses were breached.
- A Secret Service investigation and a Senate inquiry are underway.
- So even though no actual “PII” was lost, millions of breach notifications were made.

EPSILON BINGO				
1800-Flowers	American Express	Ameriprise Financial	Barclays Bank	Abe Books
Bebe's	Benefit Cosmetics	BestBuy	Brookstone	Capital One
Citibank				

EPSILON BINGO				
LL Bean	Marriott	McKinsey Quarterly	New York & Co	QFC
Red Roof	Ritz Carlton	Robert Half	Smith Brands	TiVo
Target	TD Ameritrade	FREE SPACE	US Bank	Viking Cruises
Walgreen	J. Crew	Citigroup	Fred Meyer	Fry's
Beach Body's	Scott Trade	TIAA CREF	Charter Comm	Verizon

Could this information be considered “personal” or PII?

- whether you are male or female
- where you were born
- your college or high school
- your height, your weight, your eye color
- the name of your pet
- your mother’s maiden name
- your favorite sports team
- your zip code
- your hobby
- your opinion



Non-traditional PII may identify you

- How many people in the U.S. share your specific combination of zip code, birth date, and sex?
- The answer is: probably no one.
- According to one study, 87% of the American population can be uniquely identified using just these three attributes.

Can we even say for sure what PII is?
Do we really know what we have to protect?

**"I don't have a bank account
because I don't know my
mother's maiden name."**

- *Paula Poundstone*

Privacy Breach Headlines

IT Project Failures
Michael Krigeman

Mobile
RSS
Email A

Home / News & Blogs / IT Project Failures

Scathing report slams UK gov't data loss

By Michael Krigeman | July 2, 2008, 7:23am GMT

Summary
guardian.co.uk

News Sport Comment Culture Business Money Life & style Travel Environment

Zurich loses personal details of 51,000 customers

Insurance firm says the data was lost during a routine transfer to South Africa in August last year, but there is so far no evidence of any misuse

Final report

HSBC Data Theft Hits 15,000 Rich Customers

Banking giant HSBC has apologised after revealing that details of 15,000 wealthy customers who held accounts with its Swiss private bank were stolen by an employee

Timeline: Child benefits records loss

Two CDs containing personal details of 25m people have been lost by HM Revenue and Customs. Here is how the crisis unfolded.

HM Revenue and Customs gives the National Audit Office's child benefit data, in breach of security information is later safely returned.

00 people's details go missing after...

Scott McNealy

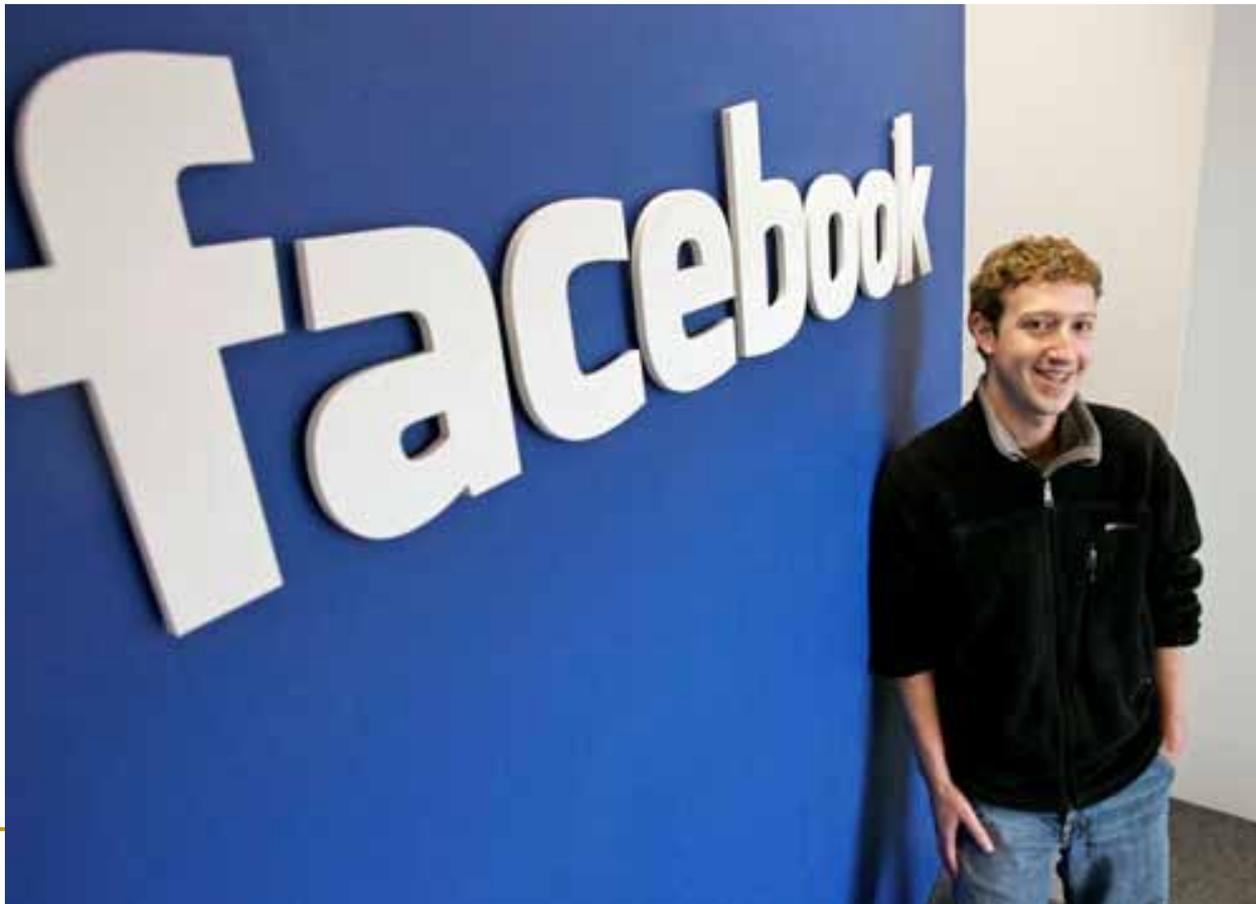
ex-CEO of the ex-Sun Microsystems (Java)

***“You have zero privacy anyway.
Get over it!”***



Mark Zuckerberg – CEO Facebook

“Privacy is no longer a social norm.”



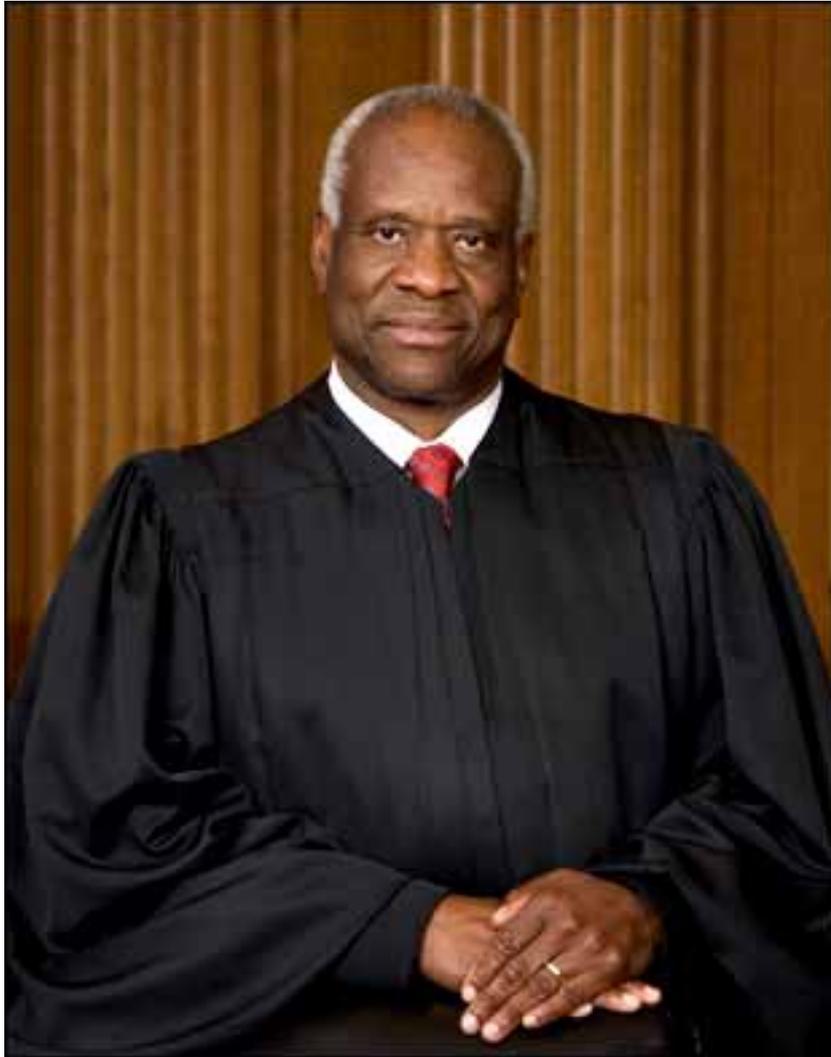
The Google logo is displayed in its characteristic multi-colored font (blue, red, yellow, blue, green, red) against a light background.

- *(Regarding personal information that can be found on Google) "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place."*
- *(People who take issue with their homes appearing on Google Street View) "can just move".*
- *"No harm, no foul." (his response when 'Street View' cars were revealed to be collecting data, images, & email from Wi-Fi that it intercepted while photographing streets & houses).*
- *(Implementing stricter privacy safeguards) "slows everything down. Ultimately, we're not going to do anything that disadvantages speed."*
- *"Google's policy is to get right up to the creepy line and not cross it."*



Eric Schmidt
Executive
Chairman of
Google

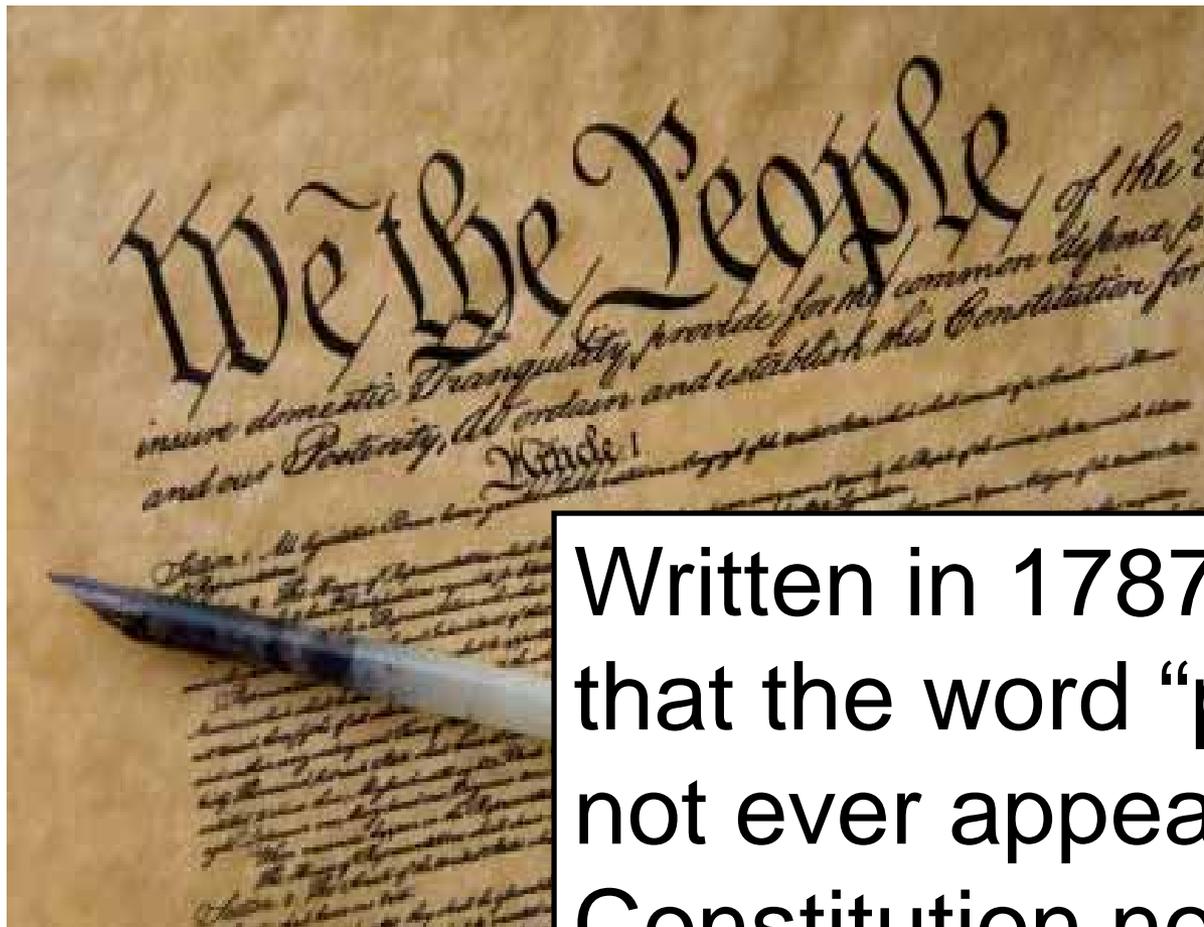
Supreme Court Justice Clarence Thomas



“...I can find neither in the Bill of Rights nor any part of the Constitution a general right of privacy...”

How do we reconcile this?

- Failures of privacy protection appear in the news on a daily basis.
- Sun, Facebook, Google & other companies have made billions of dollars selling our privacy
- But does the Constitution really not mention the right to privacy?



Written in 1787, it is true that the word “privacy” does not ever appear in the Constitution nor does it appear in the Bill of Rights (1791).

Did the Founding Fathers not care about privacy?



In an on-line search of 16,000 documents written by **Thomas Jefferson**, he never once writes the word “**privacy**”.

1787-Thomas Jefferson

While Jefferson never wrote the word “privacy”, he did write this. While in Paris serving as the Minister to France, Jefferson sent this in a report to James Madison:

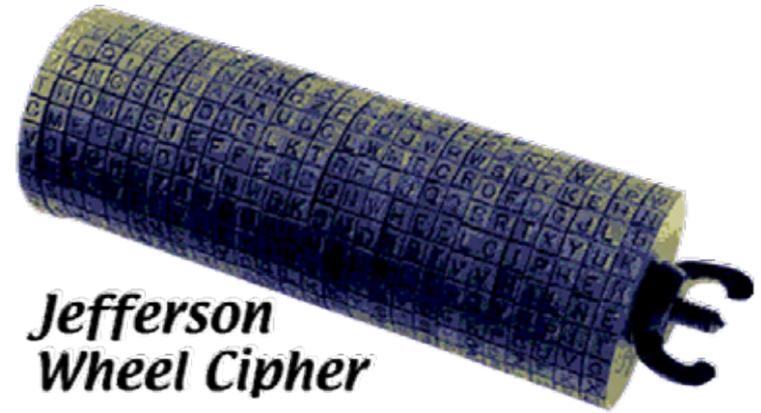


“The 1647 of 678.914 for 411.454 is 979.996.607.936. of all 789. The 404 is 747.872. And an 223.435.918 of some sort is not impossible. ... I cannot write these things in a public dispatch because they would 598 in a 1030.7.207 and 884.366.1525.”

Robert Ellis Smith. (2000)

Ben Franklin’s Web Site: Privacy and Curiosity from Plymouth Rock to the Internet.

Thomas Jefferson



When decrypted:

“The king’s passion for drink is divesting him of all respect. The queen is detested and an explosion of some sort is not impossible. ... I cannot write these things in a public dispatch because they would get in the newspaper and come back here”.

No Wiki-Leaks for TJ! -

Privacy in the 1700's

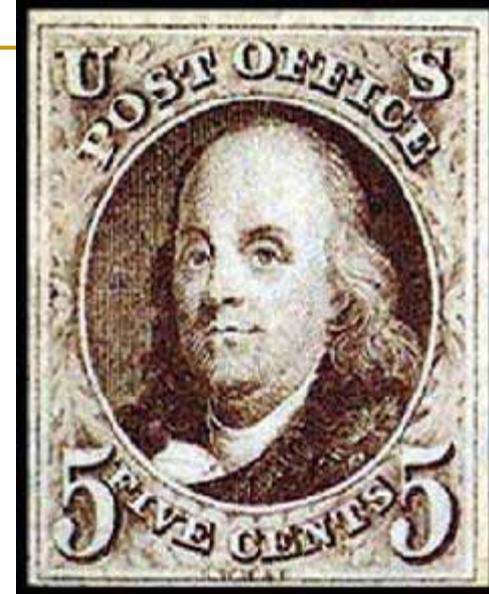
- In the vernacular of the 1700's, the word "privacy" was used a little differently.
- "Privacy" in 1787 was a code word for toilet functions. A "right to privacy" would most literally have meant the "right to go relieve yourself".
- Toilet functions typically occurred in an outhouse, which was called a "privy".



The Constitution

- “Privacy” is never mentioned in the Constitution. The popular definition of the word was different at the time.
- However, the Constitution does proscribe two different powers to the Federal Government that may demonstrate how important the concept of privacy was valued in the 1700’s.
- One of these Constitutional powers seems to protect privacy, while the other seems to take it away.
 - **Post Office & the Census**

1787 – The Constitution establishes the Post Office



- In the mid 1700's, the existing post office, was controlled by the British. The Brits routinely opened, read and censored the mail in order to squash the spread of rebellious sentiment.
- Benjamin Franklin is the 1st Postmaster General (pre-Constitution). Confidentiality of the mail becomes his number one priority.
- Article 1, Section 8, Clause 7 of the Constitution: "To establish Post Offices...";
- Federal Law: TITLE 18 / PART I / CHAPTER 83 /1703: Delay or destruction of mail or newspapers

"Whoever, without authority, **opens**, or destroys any mail or package of newspapers not directed to him, shall be fined under this title or imprisoned not more than one year, or both."

1790 - the Establishment of the Census

- Article 1 Section 2 of the Constitution establishes the *enumeration* of the people of the U.S. (a census) once a decade in order to determine Congressional representation and tax apportionment.
- Before the Revolutionary War, the British had seized birth & marriage rosters from churches in order to locate & identify revolutionary subversives. This recent history made the public immediately distrustful, uncooperative & even hostile with post-war census takers.

Early census questions were considered intrusive: Is anyone in your house deaf, blind, dumb, insane, idiotic, a pauper or a convict?

- Although it took decades, the public came around. People finally accepted the census when they realized that their anonymity was fairly well protected by the sheer volume of information that was collected.

1791-Bill of Rights



- **First Amendment** Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech,.... (privacy of beliefs?)

Fourth Amendment The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, ... (privacy of the person and possessions?)

Ninth Amendment The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people. (general protection for privacy?)

1838-Telegraph

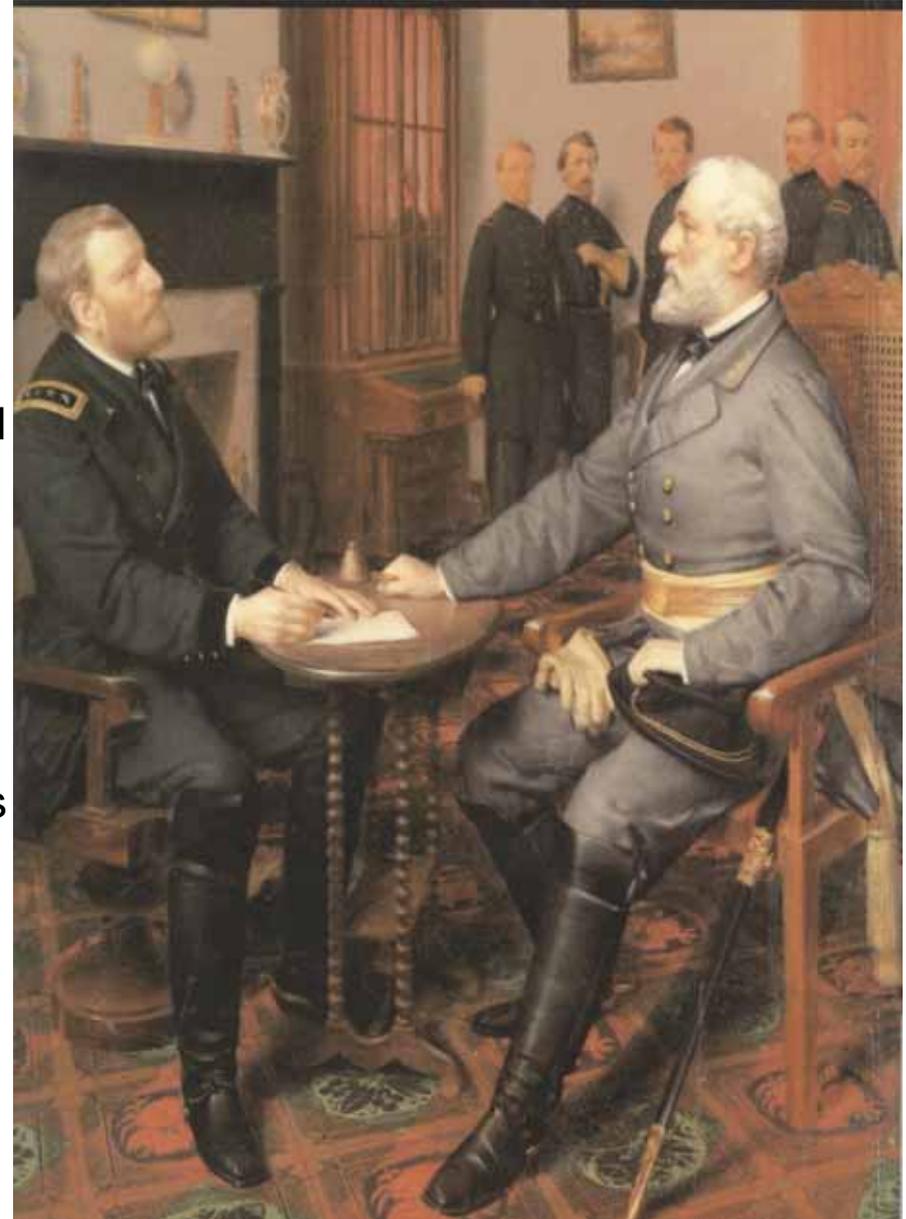


1838 - Telegraph is invented

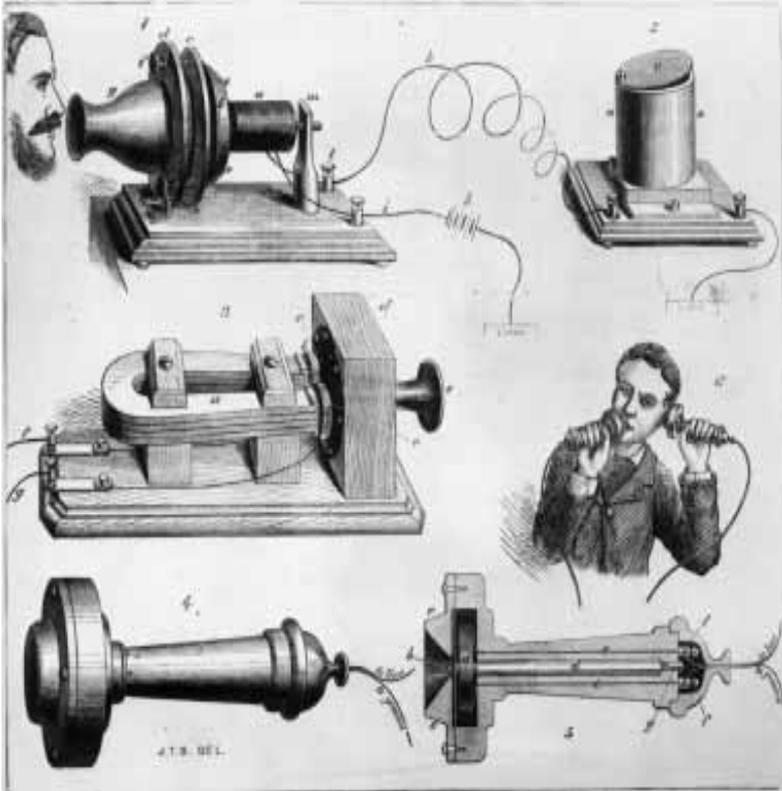
- Telegraphs revolutionized communication. Messages that used to take weeks to deliver by post now took less than a day.
- However, the nature of telegrams, required many individuals to have access to the message in order to send, route and deliver it.
- It was soon evident that the laws put into place to protect the confidentiality of mail didn't apply to telegrams.
- The wire-tapping of telegraphs begins almost immediately.

1865 – The Civil War

- April 2, 1865. U.S. Grant's Union army has seized the city of Petersburg.
- Robert E. Lee withdraws his troops from Petersburg & retreats toward Appomattox.
- Lee wires his supply depot in Lynchburg to immediately send food & ammunition by rail to Appomattox Station.
- Using a wiretap, the Union army intercepts the telegram & dispatches George Armstrong Custer to stop the train.
- Custer defeats Lee's small advance force and captures the train, keeping the supplies from reaching the Army of Northern Virginia.
- Out of food and low on ammunition, Lee tried to retake the train the next morning, but failed.
- On April 9, 1865, Lee surrendered to Ulysses S. Grant at Appomattox.



1876-Telephone



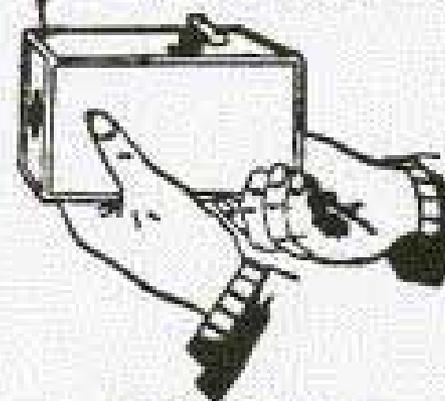
By the 1890's, law enforcement agencies were wire tapping telephone networks.

1888-Photography

In 1888, George Eastman developed the "Kodak" camera. The Kodak allowed impromptu and often clandestine "snap" photographs.

THE KODAK CAMERA

100
Instantaneous
Pictures!



Anybody can use it.
No knowledge of
photography is
necessary.

The latest and
best outfit for ama-
teurs.

Send for descrip-
tive circulars.

Price \$25.00.

The Eastman Dry Plate & Film Co.
ROCHESTER, N. Y.

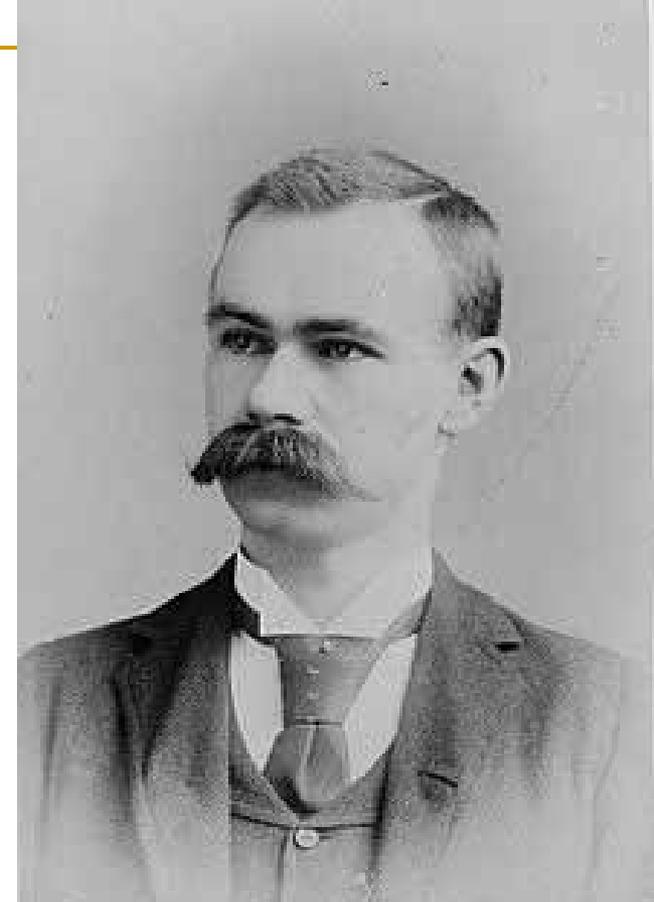
1888

1887-The Hollerith Card

- The census of 1880 took nearly 9 years to be compiled by hand.

- Herman Hollerith, a US Census Bureau clerk, invented a “tabulating machine” in 1887.

- His machines were used for the 1890 census and accomplished in less than 1 year what had taken nearly 9 years to tabulate by hand in the previous census.

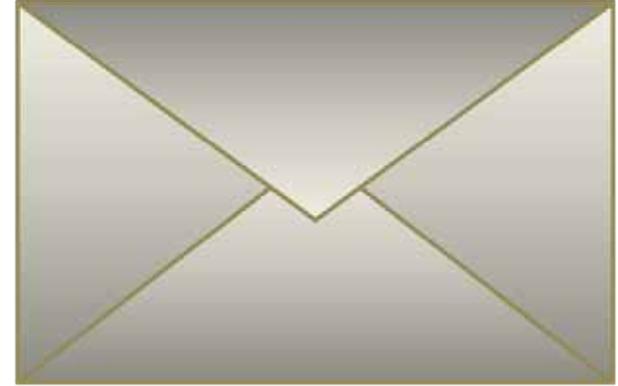


- The collection & analysis of large amounts of data was now feasible.

- In 1896, he founded the Tabulating Machine Company, which in 1924 became better known as IBM.

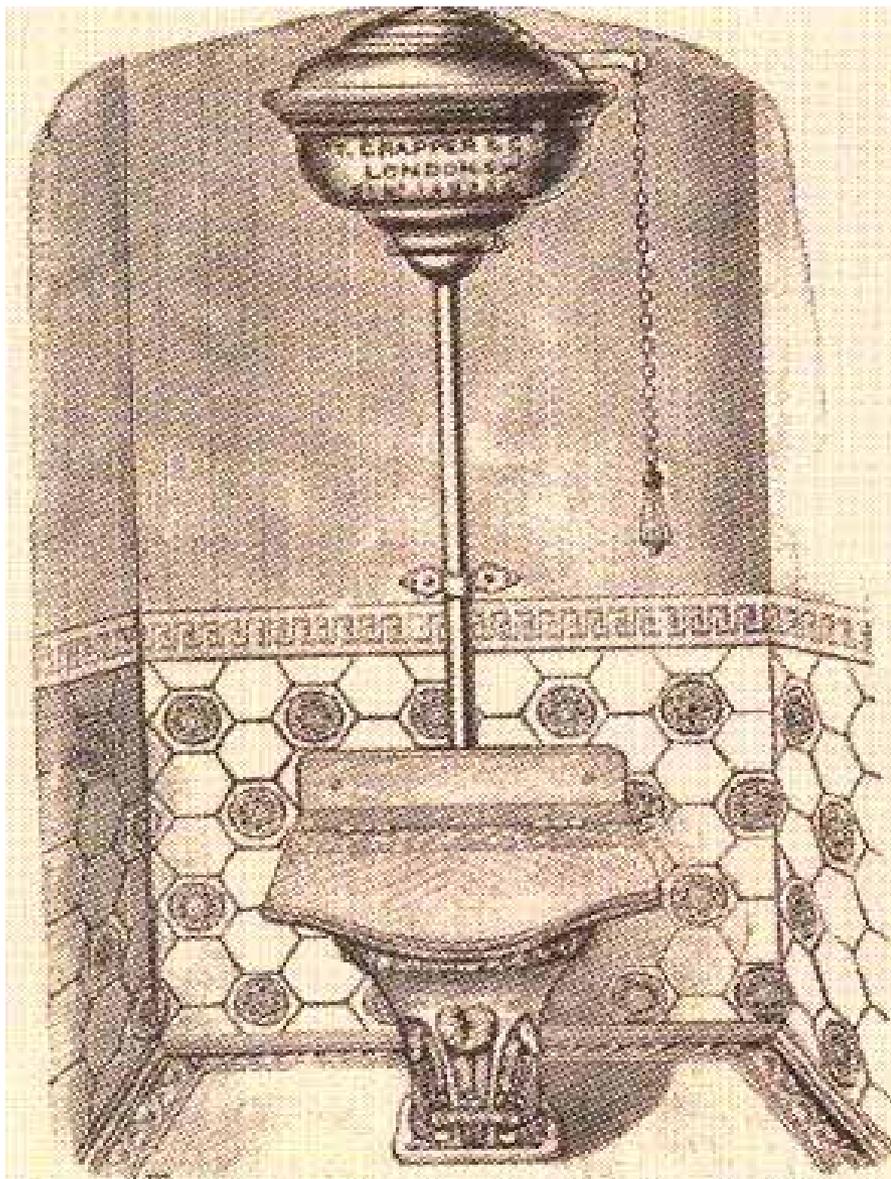
1	2	3	4	W	M	0	1	5	5	Un	0	6	12	0	6	12	Me	Nil	VI	OH	MH	IA	SD
5	6	7	8	9	F	10	15	18	6	S	1	7	13	1	7	13	MES	HR	CI	IND	WIS	MO	2899
1	2	3	4	Ch	20	21	25	30	7	MO	2	8	14	2	8	14	NY	PA	MA	ILL	MIN	ND	2899
5	6	7	8	Sp	35	40	45	50	2	MI	3	9	15	3	9	15	WV	VA	WVA	DC	TEX	ALA	CLY
1	2	3	4	In	55	60	65	70	3	Wd	4	10	16	4	10	16	DE	NC	SC	MS	LA	ARK	WJH
5	6	7	8	75	80	85	90	95	4	Jn	5	11	17	5	11	17	DE	PA	VA	DC	LA	ARK	WJH
1	2	3	4	Er	OK	0	4	17	11	5	Un	15	2	0	15	2	US	Un	En	US	Un	En	VIA
5	6	7	8	Oh	NR	1	5	01	12	6	NG	20+	3	1	Gr	Ir	Sc	Gr	Ir	Sc	AM	2899	
1	2	3	4	2	NW	4	6	0	13	7	1	Na	4	7	Sw	CE	Wc	Sw	CE	Wo	WVO	2899	
5	6	7	8	4	0	7	4	7	1	14	8	2	Pa	5	Sz	Nw	CP	Fu	Nw	CP	HJ	2899	
1	2	3	4	6	12	10	6	8	2	15	9	3	A	6	Po	Bx	Fr	II	Dx	Fr	II	2899	
5	6	7	8	8+	Un	g	f	9	3	16	10	4	Un	0	01	Ru	Bu	01	Ru	Bu	Sz	34	

1891 - Envelope Seal



- Inventor Frank W. Leslie patents the “envelope seal”
- Unlike wax seals, these new envelopes make mail tampering much more difficult to conceal.
- The invention further ensures the confidentiality of “sealed” mail & was reinforced by numerous court cases.
- The Supreme Court rules that mailed letters are entitled to Fourth Amendment protection against unreasonable search & seizures.

1894 - Flush Toilet



CRAPPER'S

Improved

Registered Ornamental

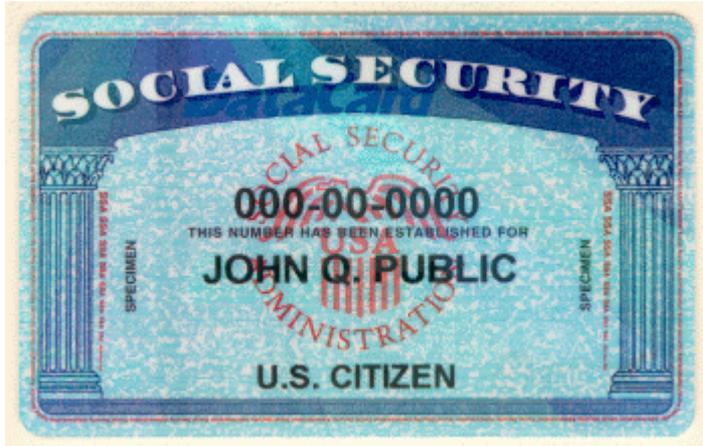
Flush-down W.C.

With New Design Cast-iron Syphon Water
Waste Preventer.

No 518.

Improved Ornamental Flush-down W.C. Basin
(Registered No. 145,823), Polished Maho-
gany Seat with flap, New Pattern 3-gallon
Cast-iron Syphon Cistern (Rd. No. 149,284),
Brass Flushing Pipe and Clips, and Pendant
Pull, complete as shown £6 15 0

1936 Social Security Numbers



- In 1936, the Social Security Administration assigns an identification number to most adult Americans.
- In 1943, FDR requires Federal agencies to use SSN as an identifier in any NEW “systems of records”.
- In 1961, the IRS begins using SSN as a taxpayer identifier.
- In 1969, the Pentagon began to use SSN as a military ID. GI gear is routinely tagged or even spray painted with the soldier’s SSN.
- In 1970, the Bank Secrecy Act required banks to obtain SSN as proof of identity. As a convenience for themselves, banks start printing SSN’s on the face of all checks.
- In the 1970’s most state DMVs require SSN to get a driver’s license & many are using SSN’s as a driver’s license #.
- In the 1970’s, most colleges are beginning to use SSN as a student ID.
- In the 70’s & 80’s, insurance companies & other private businesses are using SSN to identify customers.
- In 1986, the IRS requires all dependents claimed on a tax return, including minor children, to also have a SSN.
- In 1987, 7 million fewer dependents were claimed on IRS tax returns.



**How do we
put the SSN
cat back in the
bag?**

Virginia FOIA (has the solution?)

- § 2.2-3815. Access to social security numbers prohibited; exceptions
- A. Except as otherwise provided in this chapter, the first five digits of a social security number contained in a public record shall be confidential and exempt from disclosure under the Freedom of Information Act (§ 2.2-3700 et seq.).

Decoding Social Security Numbers in One Step

[Stephen P. Morse](#), San Francisco

Structure of SS Numbers

My Other Webpages

Three-Digit Decoder

SSN starting with - XX - XXXX

was issued in

Where card was issued, not where person was born

Five-Digit Decoder

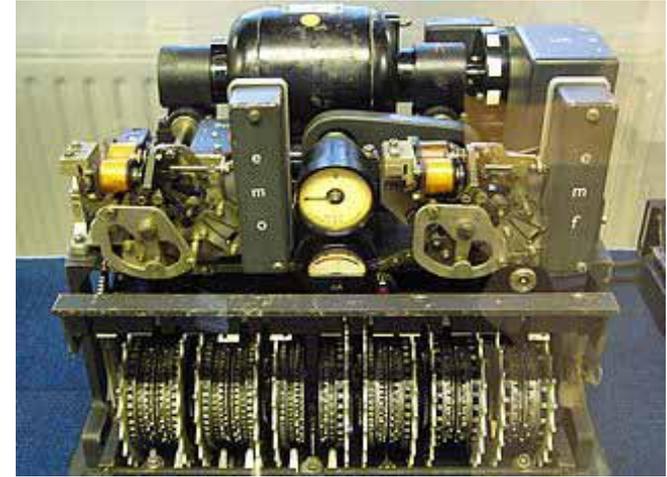
SSN starting with - - XXXX

was issued in 229-21: Virginia, 1980

Where and when card was issued, not where and when person was born

1941-45 World War II

- Cryptography had tremendous military value and made an enormous impact on WWII. After the war, the US passed numerous laws to regulate the export of cryptography for national security purposes.



1950's Surveillance

- Public trust in the government was at an all-time high after the war.
- Paranoia over communists and subversives infiltrating the country was also at an all-time high.
- Government surveillance on private citizens grew rapidly.



1965 – James Bond

The popularity of James Bond & “Get Smart” led to a public fascination with miniaturized devices in the 1960’s. In a 1965 Senate Committee hearing on privacy, a man demonstrated how a miniature listening device could be hidden in an everyday object, such as an olive in a martini.

One Senator asked, “Does it only work with gin or will it also work with vodka?”



1960’s-1970s: Information Technology

- Commercial Databases
- Open Data Exchange Standards
- Data Exchange Methods (i.e. networks)
- **Exponentially** increasing amounts of data





FOIA (1966)

Opens government data records to public scrutiny. (The public's right to know.)



PRIVACY ACT (1974)

Requires security procedures to protect the confidentiality of data. (To protect an individual's privacy.)

1975 - Personal Computers

- In 1975, personal computers become commercially available.
- In 1981, IBM introduces the IBM PC which creates a revolution in information technology.



1977-Birth of Modern Identity Theft



- George Turner, incarcerated for tax fraud, was given a prison job sorting through discarded military clothing.
- The clothes were tagged with the names and SSN's of soldiers.
- Turner used the information on the tags to file over 200 false tax returns for refunds with the IRS.
- By the end of the 1990's, identity theft had become one of the fastest growing crimes in the world.

1989- World Wide Web

- Email
- Cookies
- E-Commerce
- Wireless



The WWW revolutionizes communication, business and personal lives. It created more privacy issues in a shorter amount of time & on a larger scale than perhaps any other technological innovation before or since.

Two Faces of Web Site Privacy

1. Privacy of individuals whose personal data may be available on a website.
2. Privacy of users who visit our web sites.

2003 - § 2.2-3803. Administration of systems including personal information; Internet privacy policy;

B. Every **public body**, as defined in § 2.2-3701, that has an Internet website associated with that public body **shall develop an Internet privacy policy** The statement shall be made available on the **public body's website in a conspicuous manner**. ...

www.virginia.gov's Privacy Policy

Use of "Cookies"

. . . . Any application or web page that uses cookies will identify itself as such. . . . No user information is gathered through cookies except for that needed to run the specific application.

Restrictions on the disclosure of customer information

... We do not reveal specific information about subscribers or other personally identifiable data to unaffiliated third parties for their independent use

P3P

Platform for Privacy Preferences Project

From www.virginia.gov's privacy policy:

“The Virginia portal continues to be P3P compliant.”

P3P

The Platform for Privacy Preferences (P3P) was created ... to make it easier for website visitors to obtain information about a site's privacy policy. **P3P specifies a standard XML format for machine-readable privacy policies that can be parsed by a P3P enabled browser.** When a user encounters a P3P website policy that does not conform to the user's preferences, the browser can alert the user or take other actions such as blocking cookies.

Typical privacy policy

P3P enabled privacy policy

Designed to be read by a human

Designed to be read by a computer

Can contain fuzzy language and may be even be ambiguous

Multiple choice questions – sites must place themselves in one “bucket” or another

Can include as much or as little information as a site wants

Must include disclosures in every required area

Easy to provide detailed explanations

Limited ability to provide detailed explanations

Sometimes difficult for users to determine boundaries of what it applies to and when it might change

Boundaries are precisely scoped

Web site controls presentation

User agent (or P3P browser) controls presentation

Table by Dr. Lorrie Cranor

P3P Experiment

- Obtained a list of 298 COV websites.
- Randomly sampled 30 for compliance with the COV website privacy policy (§ 2.2-3803).
- 19 of the 30 (63%) websites were confirmed to have a privacy policy in a “conspicuous” location.
- 11 websites (37%) in the sample do not appear to have a privacy policy at all.
- Only 3 (10%) of the websites sampled were found to be using a P3P compliant privacy policy.

Privacy Report



Based on your privacy settings, no cookies were restricted or blocked.

Show:

Websites with content on the current page:

Site	Cookies
http://widgets.twimg.com/j/2/widget.js	
http://s7.addthis.com/js/250/addthis_widget.js#use...	
http://s7.addthis.com/static/r07/widget53.css	
http://www.google-analytics.com/ga.js	
http://206.113.151.152/accuweather/html/RIC.js	
http://www.virginia.gov/images/virginia_dot_gov_lo...	
http://www.virginia.gov/images/common_feel_bg.jpg	
http://www.virginia.gov/cmsportal3/images/spacer.gif	

To view a site's privacy summary, select an item in the list, and then click Summary.

Summary

[Learn more about cookies](#)

Settings

Close

When you visit www.virginia.gov; these are some of the companies that are in turn visiting you:

- **twimg.com (twitter)**
- **addthis.com (clearspring)**
- **google-analytics.com (google)**
- **fbcdn.net (facebook)**
- **getclicky.com (roxr)**
- **amazonaws.com (amazon)**

None of the privacy policies for these websites are P3P compliant, so therefore, none of the policies can be read from www.virginia.gov.

Per Google Analytics: Recommended Addition to Privacy Policy

“This website uses Google Analytics, ... Google Analytics uses “cookies”, The information generated by the cookie about your use of the website (including your IP address) will be transmitted to and stored by Google Google will use this information for ... evaluating ..., compiling reports on website activity ... & providing other services relating to website activity and internet usage. Google may also transfer this information to third parties By using this website, you consent to the processing of data about you by Google ...”

1996- HIPAA



- Virginia § 32.1-127.1:05. (Effective 1/1/2011) Breach of medical information notification.

■ Health Insurance Portability Accountability Act

- HIPAA Privacy rule goes into effect in 2003
- Until 2003, the Video Privacy Protection Act (1988), meant that your video rental records had more legal privacy protection than your medical records.
- HHS did not assess a single civil penalty for the first 5 years of the privacy rule, in spite of over 30,000 complaints. The first penalty was in July 2008 for \$100,000.

1999 – Identity Theft



Identity Theft

In 1999, the Federal Trade Commission (FTC) first listed **identity theft** as the number one consumer complaint. In March 2011, the FTC once again named identity theft as the top complaint for the year 2010, the 11th year in a row.

The most common form of identity theft was through **fraudulent government documents.**



Todd Davis

CEO of Lifelock, Inc.

- Lifelock promised in ads that its \$10 monthly service would protect consumers from identity theft.
- Todd Davis, Lifelock CEO, prominently displayed his personal SSN in TV commercials, print ads, websites, billboards & on the side of a truck that was driven around the country as a promotional gimmick.
- In March 2010, the company was fined \$12 million by the Federal Trade Commission for deceptive advertising.
- By May 2010, Todd Davis's identity had been stolen 13 times

2004

Social Networking



- 96 % had posted their birthday
- 85% had posted their email address
- 85% had posted their hometown
- 81% their relationship status
- 72% posted the school they attended
- 24% posted their phone #
- 25% had posted a picture they would not want an employer to see.
- 27% feel that other people had posted defaming information about them.
- 35% feel they could never be in politics due to damaging personal information about them online.
- Only 4% posted their home address

Mark Zuckerberg is right: social norms are changing.

~ 2005 Location Based Services



Cell phone triangulation, GPS, IP address tracking, surveillance cameras, transponders, RFID, License Plate Readers & “geo-tagged” digital images, are increasing the capability to determine not only the physical location of a device, but also the person using the device (or targeted by the device).

- **Your “location” says a lot about you:**
 - **Where you go / What you do / Who you meet**
- **GPS can be accurate to within 30 feet. Some IP tracking can be even more precise.**
- **Location tracking has been used to:**
 - **To track fleet vehicles / To provide mapping assistance / Deliver restaurant recommendations / Provide targeted advertising content / By police to track drug traffickers and other criminals.**
- **It can also be used to track cheating husbands or stalk ex-girlfriends.**

What if you were on your cell phone & driving by a convenience store at about the time that it was being robbed? You may be a suspect.

2010-TSA Full Body Scanners



2011- FTC Do Not Track

- A study by the WSJ revealed that the nation's 50 top websites installed, on average, 64 pieces of tracking technology onto the computers of visitors in the form of cookies, Flash cookies & “beacons”.
- FTC has proposed a “do not track” regulation.
- Consumers will be able to “opt out” of any technology that monitors what they do on the internet.
- Opponents counter that behavioral tracking technologies bring in over \$300 billion per year to the U.S. economy.



2011 - Privacy Bill of Rights

- March 2011, the Obama Administration has called for Congress to enact legislation to create a consumer privacy bill of rights that would regulate the collection and use of personal data on the Internet.
- There are also numerous other privacy legislation bills being considered.

What are some of the other privacy issues that are already out there & waiting to be addressed?

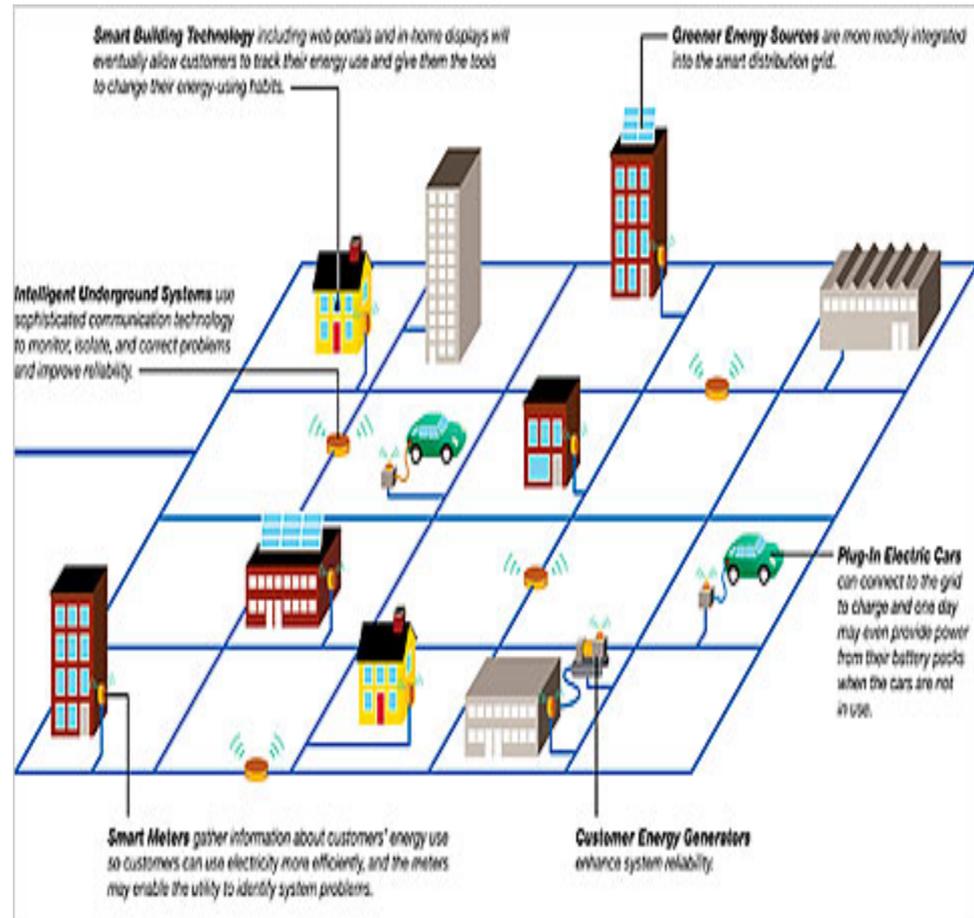
Cloud

- When data is stored on someone else's hardware, the responsibility for protecting that information from hackers and internal data breaches falls into the hands of the custodian rather than the data owner. Remember Epsilon!



Smart Grid

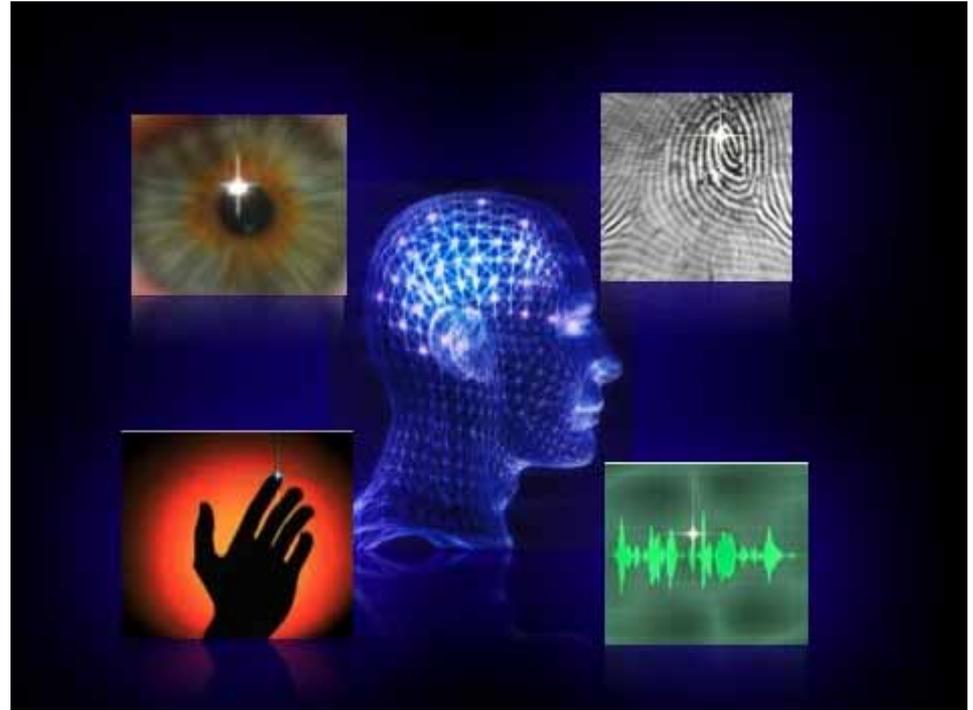
- Smart grids monitor the energy consumption patterns in your home to help determine when power usage should be limited.
- As a result, the grid “knows” when the home is occupied & what activities are going: TV is on, clothes are being washed, shower, lawn watering, cooking, thermostat, etc.



What if smart grid data were sold, subpoenaed, or stolen?

Biometrics

Fingerprints
Retina Scanning
DNA
Voice prints
Facial Recognition



- **Unauthorized secondary uses (function creep)**
- **Expanded surveillance and profiling of individuals**
- **Data misuse (including identity theft)**
- **False matches, non-matches, and system errors.**

Significant data security risks include potential spoofing, tampering, various security attacks, and insufficient accuracy.

Video Surveillance

- **Video cameras are cheap & they are everywhere**
- **Typically requires no notice or consent.**
- **Are we creating a generation of people who are becoming used to being watched?**
- **How long before simple surveillance cameras evolve into facial recognition cameras?**



Data Profiling

- **Is your data “you”?**
 - **We leave a digital trail everywhere we go:**
 - **Credit cards record date, time and item purchased**
 - **Websites record where you went, what you clicked, what you downloaded, what you keyed, etc.**
 - **Your car’s “e-z-pass” is used to automatically debit your account & record the date, time & location of the toll.**
 - **Mobile devices may be recording your location even without you realizing it.**
 - **Retailer discount cards create a database of what you bought from a store.**
-

What do we do?



Laptop CompuBody Sock
<http://sternlab.org/2008/04/body-technology-interfaces>

Generally Accepted Privacy Principles

1. **Manage it, i.e. make someone accountable**
2. **Provide notice**
3. **Obtain consent**
4. **Collect only for the intended purpose (*when in doubt, leave it out*)**
5. **Define usage limitations, retention & disposal**
6. **Allow access, review & correction**
7. **Disclose to 3rd parties only with consent**
8. **Secure it! (*if you collect it, you must protect it*)**
9. **Maintain quality**
10. **Continuously monitor**



Risk assessments should address these principles.



***PRIVACY* must be part of a
comprehensive *SECURITY*
program.**

**The
End?**

References

- Robert Ellis Smith. (2000) *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet*.
- Lorrie Cranor. (2007) Director of *Cylabs Usable Privacy and Security Laboratory (P3P)* (Carnegie Mellon University).
- Thom Hartman. *The Rights of Citizens of the United States Are in Jeopardy*
- AICPA. (2009) *Generally Accepted Privacy Principles*.
- Privacy Rights Clearinghouse. (2001, rev. 2011) *Privacy Today: A Review of Current Issues*.
- Daniel Solove, Paul M. Schwartz (2009) *Privacy, Information and Technology*.

Other Privacy Sources

- American Civil Liberties Union, www.aclu.org
- Electronic Frontier Foundation, www.eff.org
- Electronic Privacy Information Center, www.epic.org
- Health Privacy Project, www.healthprivacy.org
- Federal Trade Commission,
<http://www.ftc.gov/opa/2010/12/privacyreport.shtm>
- National Consumers League, www.nclnet.org
- Privacy Activism, www.privacyactivism.org
- Privacy Rights Clearinghouse, www.privacyrights.org
- U.S. Public Interest Research Group, USPIRG,
www.pirg.org



Virginia Information Technologies Agency

Personnel Security: A short review of SEC 501-01

Bob Baskette

Senior Manager, Security Operations
and Architect



SEC 501 8.1

Personnel Security

- Purpose
 - Personnel Security requirements delineate the steps necessary to restrict access to IT systems and data to those individuals who require such access as part of their job duties.



SEC 501 8.1

Personnel Security

- Purpose
 - This component of the COV Information Security Program defines requirements in the following four areas:
 - Access Determination and Control
 - Information Security Awareness and Training
 - Acceptable Use
 - Email Communications



SEC 501 8.2

Access Determination and Control

- Purpose
 - Access Determination and Control requirements identify the steps necessary to restrict access to IT systems and data to authorized individuals.



SEC 501 8.2

Access Determination and Control

- Requirements
 - 1. Perform background investigations of all internal IT System users based on access to sensitive IT systems or data. Existing users may be grandfathered under the policy and may not be required to have background investigations.
 - Note: Agencies should consult the Code of Virginia § 2.2-1201.1 and Department of Human Resource Management (DHRM) Policy 2.10.



SEC 501 8.2

Access Determination and Control

- Requirements
 - 2. Restrict visitor access from facility areas that house sensitive IT systems or data.
 - 3. Require non-disclosure and security agreements for access to IT systems and data, based on sensitivity and risk.



SEC 501 8.2

Access Determination and Control

- Requirements
 - 4. Remove physical and logical access rights upon personnel transfer or termination, or when requirements for access no longer exist, as required in Section 5.2 and Section 7.2.
 - 5. Establish termination and transfer practices that require return of agency logical and physical assets that provide access to sensitive IT systems and data and the facilities that house them.



SEC 501 8.2

Access Determination and Control

- Requirements
 - 6. Temporarily disable physical and logical access rights when personnel do not need such access for a prolonged period in excess of 30 days because they are not working due to leave, disability or other authorized purpose.
 - 7. Disable physical and logical access rights upon suspension of personnel for greater than 1 day for disciplinary purposes.



SEC 501 8.2

Access Determination and Control

- Requirements
 - 8. Establish separation of duties in order to protect sensitive IT systems and data, or establish compensating controls when constraints or limitations of the agency prohibit a complete separation of duties. Example: Such compensating controls may include increased supervisory review; reduced span of control; rotation of assignments; independent review, monitoring, and/or auditing; and timed and specific access authorization with audit review, among others.



SEC 501 8.2

Access Determination and Control

- Requirements
 - 9. Explicitly grant physical and logical access to sensitive IT systems and data and the facilities that house them based on the principle of least privilege.



SEC 501 8.3

Information Security Awareness and Training

- Purpose
 - Security Awareness and Training requirements identify the steps necessary to provide IT system managers, administrators, and users with awareness of system security requirements and of their responsibilities to protect IT systems and data.



SEC 501 8.3

Information Security Awareness and Training

- Requirements
 - 1. Include any agency-specific information security training requirements in the agency information security awareness and training program.
 - Example: An agency that processes data covered by the Health Insurance Portability and Accountability Act (HIPAA) must have an information security awareness training program that addresses specific HIPAA data security requirements.



SEC 501 8.3

Information Security Awareness and Training

- Requirements
 - 2. Require that all IT system users, including employees and contractors, receive information security awareness training annually, or more often as necessary. Generally, best practice is that annual security awareness training lasts at least one hour.



SEC 501 8.3

Information Security Awareness and Training

- Requirements
 - 3. Require additional role-based information security training commensurate with the level of expertise required for those employees and contractors who manage, administer, operate, and design IT systems, as practicable and necessary.
 - Example: Agency employees and contractors who are members of the Disaster Recovery Team or Security Incident Response Team require specialized training in these duties.



SEC 501 8.3

Information Security Awareness and Training

- Requirements
 - 4. Implement processes to monitor and track completion of information security training.
 - 5. Require information security training before (or as soon as practicable after) IT system users receive access rights to the agency's IT systems, and in order to maintain these access rights.



SEC 501 8.3

Information Security Awareness and Training

- Requirements
 - 6. Develop an information security training program so that each IT system user is aware of and understands the following concepts:
 - a. The agency's policy for protecting IT systems and data, with a particular emphasis on sensitive IT systems and data;
 - b. The concept of separation of duties;



SEC 501 8.3

Information Security Awareness and Training

- Requirements
 - 6. cont.
 - c. Prevention and detection of information security incidents, including those caused by malicious code;
 - d. Proper disposal of data storage media;



SEC 501 8.3

Information Security Awareness and Training

- Requirements
 - 6. cont.
 - e. Proper use of encryption;
 - f. Access controls, including creating and changing passwords and the need to keep them confidential;



SEC 501 8.3

Information Security Awareness and Training

- Requirements
 - 6. cont.
 - Note: It is considered best practice not to base passwords on a single dictionary word. It is strongly recommended that system users be educated not to base passwords on a single dictionary word.



SEC 501 8.3

Information Security Awareness and Training

- Requirements
 - 6. cont.
 - g. Agency acceptable use policies;
 - h. Agency Remote Access policies;
 - i. Intellectual property rights, including software licensing and copyright issues;



SEC 501 8.3

Information Security Awareness and Training

- Requirements
 - 6. cont.
 - j. Responsibility for the security of COV data;
 - k. Phishing; and
 - l. Social engineering.



SEC 501 8.3

Information Security Awareness and Training

- Requirements
 - 6. cont.
 - Note: Over a period of not more than two years, security awareness training should include the concepts above based on the needs of the agency relative to the sensitivity of the agency's data and IT systems.



SEC 501 8.3

Information Security Awareness and Training

- Requirements
 - 7. Require documentation of IT system users' acceptance of the agency's security policies after receiving information security training.



SEC 501 8.4 Acceptable Use

- Purpose
 - Acceptable Use requirements identify the steps necessary to define acceptable and permitted use of IT systems.



SEC 501 8.4 Acceptable Use

- Requirements
 - 1. Document an agency acceptable use policy. Executive branch agencies must adhere to Virginia Department of Human Resource Management (DHRM) Policy 1.75 – Use of Internet and Electronic Communication Systems. Each Executive branch agency shall supplement the policy as necessary to address specific agency needs.
 - Note: This policy can be found at http://www.dhrm.virginia.gov/hrpolicy/policy/pol1_75.pdf.



SEC 501 8.4 Acceptable Use

- Requirements
 - 2. Direct the proper use of encryption for transmitting sensitive data.
 - 3. Direct the use of an agency authorized COV warning banner to communicate that IT systems and their use may be monitored and viewed by authorized personnel; and there is no expectation of privacy when using a Commonwealth IT system.



SEC 501 8.4 Acceptable Use

- Requirements
 - 4. Require acknowledgement that monitoring of IT systems and data may include, but is not limited to, network traffic; application and data access; keystrokes (only when required for security investigations and approved in writing by the Agency Head); and user commands; email and Internet usage; and message and data content.



SEC 501 8.4 Acceptable Use

- Requirements
 - 5. Prohibit users from:
 - a. Installing or using proprietary encryption hardware/software on Commonwealth systems;
 - b. Tampering with security controls configured on COV workstations;



SEC 501 8.4 Acceptable Use

- Requirements
 - 5. cont.
 - c. Installing personal software on a Commonwealth system;
 - d. Adding system hardware to, removing system hardware from, or modifying system hardware on a COV system; and



SEC 501 8.4 Acceptable Use

- Requirements
 - 5. cont.
 - e. Connecting non-COV devices to a COV IT system or network, such as personal computers, laptops or handheld devices, except in accordance with the current version of the Use of Non-Commonwealth Computing Devices to Telework Standard (COV ITRM Standard SEC511).



SEC 501 8.4 Acceptable Use

- Requirements
 - 6. Prohibit the storage, use or transmission of copyrighted and licensed materials on COV systems unless the COV owns the materials or COV has otherwise complied with licensing and copyright laws governing the materials.
 - 7. When connected to internal networks from COV guest networks or non-COV networks, data transmission shall only use full tunneling and not use split tunneling.



SEC 501 8.4 Acceptable Use

- Requirements
 - 8. Require documentation of IT system users' acceptance of the agency's Acceptable Use Policy before, or as soon as practical after, gaining access to agency IT systems.



SEC 501 8.5

Email Communications

- Purpose
 - Email shall not be used to send sensitive data unless encryption is used. As stated in the Encryption section of this Standard, encryption may be required for the transmission of data that is sensitive relative to confidentiality and integrity. The ISO should consider and plan for the issue of agency email being intercepted, incorrectly addressed, or infected with a virus. An email disclaimer is a set of statements that are either pre-pended or appended to emails.



SEC 501 8.5

Email Communications

- Purpose
 - These statements are frequently used to create awareness of how to treat the data in the email. An email disclaimer is not a substitute for judgment on what content to put into an email.



SEC 501 8.5

Email Communications

- Requirements
 - 1. Require encryption for the transmission of email and attached data that is sensitive relative to confidentiality or integrity; however, digital signatures may be utilized for data that is sensitive solely relative to integrity as stated in the encryption component of this Standard. The ISO should consider and plan for the issue of agency email being intercepted, incorrectly addressed, or infected with a virus.



SEC 501 8.5

Email Communications

- Requirements
 - 2. Consult with the agency's legal counsel before adopting an email disclaimer. Emails sent from Commonwealth systems are public records of the Commonwealth of Virginia and must be managed as such.



Sample email disclaimer

- The information in this email and any attachments may be confidential and privileged. Access to this email by anyone other than the intended addressee is unauthorized. If you are not the intended recipient (or the employee or agent responsible for delivering this information to the intended recipient) please notify the sender by reply email and immediately delete this email and any copies from your computer and/or storage system.*



Sample email disclaimer cont.

- The sender does not authorize the use, distribution, disclosure or reproduction of this email (or any part of its contents) by anyone other than the intended recipient(s). No representation is made that this email and any attachments are free of viruses. Virus scanning is recommended and is the responsibility of the recipient.*

Questions???

For more information, please contact:
CommonwealthSecurity@vita.virginia.gov



Thank you!



Virginia Information Technologies Agency

Upcoming Events





Information Security System Association

ISSA

DATE: Wednesday, May 11, 2011

LOCATION: Maggiano's Little Italy

11800 West Broad Street, #2204, Richmond, VA 23233

TIME: 11:30 - 1:00pm. Presentation starts at 11:45.

Lunch served at 12.

COST: ISSA Members: \$20 & Non-Members: \$25

SPEAKER: Hart Rossman, VP & CTO for
Cyber Security Services & Solutions at SAIC

TOPIC: *Security in the App Store Ecosystem*



CISSP Training

Where: VDOT

When: May 16 – 20 (Training)

May 21 (Cert. Test)

Cost: \$1595 Training

\$549 Test

Need more info? Contact:

James.Austin@VDOT.Virginia.Gov



Internet Security Training Workshop

Virginia Tech & SANS Institute offer this 6-day SANS program focused on
Network Penetration Testing

May 17 – 22, 2011

*Torgersen Hall at Virginia Tech
Blacksburg, VA*

<http://www.cpe.vt.edu/isect/>

Who Should Attend:

- *Penetration testers*
- *Auditors who need to build deeper technical skills*
- *Security personnel whose job involves assessing target networks & systems to find security vulnerabilities*

- **Special pricing is available for any faculty/staff from any accredited EDU site (K-12, community college or higher education institution) or member of law enforcement.**

- * * **If you wish to receive additional information about this program, please contact Randy Marchany, IT Security Lab, Virginia Tech by e-mail at marchany@vt.edu**



MS-ISAC

National Webcast Initiative

Wednesday, June 22
2:00 pm – 3:00 pm EDT

Topic: *Federal Cyber Security Initiatives for State and Local Governments*

Visit MS-ISAC web for more information:

<http://www.msisac.org/webcast/>



Future IS Orientation Sessions

Tuesday - May 10, 2011
(CESC)

9:00 – 11:30a

Tuesday - July 12, 2011
(CESC)

1:00 – 3:30p

IS Orientation is now available via webinar!



Future ISOAG's

From 1:00 – 4:00 pm at CESC

Wednesday - June 1, 2011

Wednesday - July 6, 2011

ISOAG will be held the 1st Wednesday of each month in 2011



ISOAG-Partnership Update

*IT Infrastructure Partnership Team
Bob Baskette*

May 4, 2011



NORTHROP GRUMMAN

ADJOURN

THANK YOU FOR ATTENDING

