
ISSA
CHATTANOOGA
August 6, 2013


Why are all US Information Assurance professionals set up for failure?
What has to change for us to ever be secure.

Quick Review of February

- *By 2020 there will be 20 billion endpoints on the internet.*
- *By 2050 there will be 1 trillion.*
- *Soon your car will automatically take you to Mapco on the way home because your refrigerator told your car it needs milk.*
- *Currently there are over 3800* versions of just Android in use…is your MDM up to that?*
- *17 million mobile devices are lost in taxi's alone in any one year.*

Review

- *How long does it take to remove a SIM card?*
- *How long to remove an SD memory card?*
- *If you have only looked away from your mobile device for even three minutes…is it still secure?*
- *How about Sidetracking?*
- *Has your SIM been in your possession constantly? Are you sure?*
- *Is your Bluetooth on? Examples*
- *Has your data been captured while you had legitimate use of it?*
- *Has someone from your company decommissioned an old BYOD without clearing data properly?*

Can you be sure…

- ***Users of your data have not:***
  - ***Printed your data***
  - ***Forwarded your data,*** ***email, drop box***
  - ***Posted your data,*** ***Facebook, twitter***
  - ***Made screen shots of your data***
  - ***Saved it to a SD card, USB drive***
  - ***Allowed someone else to remove it on a SIM or SD***
  - ***Synced their Mobile device to their home computer***
- ***So have you lost control??? YES***

MDM or TDM

- *Provides a platform for you to manage all mobile devices attaching to your network.*
- *Our goal is to manage data not devices*
- *To manage data we have to be device agnostic*
- *What if the cloud loses data?*
- *Is there the potential to force a breach?*
- *What if another company forces a breach of your data?*

Reality Check

You must maintain complete control of your data from creation to destruction. DoJ

You can delegate tasks and duties but never responsibility. DoD

No responsible party has ever reported any problems with any cyber attack, all they need is time and money. Gartner

Anything on the end of an IP address is vulnerable. Lockheed

Legal Issues

- *Can you produce <u>all</u> your data in discovery?*
- *Will your operations violate hold orders?*
- *Can you be sure where your data is stored?*
- *Is it compliant? Location, encryption, controlled*
- *How much data is mobile adding to your Data store? Backup, production, control*
- *How much more does your legal staff now need to defend? Company and personal data*
- *None of this has yet been tested in a court room. hmmmmm*

US Federal Appeals Court Decision

- ***Defendant DID have a reasonable expectation of privacy:***
- ***Despite the logon banner which said otherwise.***
- ***Because the email sits behind a password only she knows.***
- ***Regardless of what was in the emails, or on the PC.***
- ***Court gave the HS Locker example***
- ***"EOP depends on the facts and circumstances at the time" *******
- ***"EOP is equal to that which "society is willing to accept as reasonable" *******

*** So where are we? ***

It's also true that those who would give up privacy for security are likely to end up with neither.

There is no security without privacy.

And liberty requires both security and privacy.

Ben Franklin

Fast Forward – This Year

- *"We cannot expect to have 100% privacy and 100% security at the same time"* *Barack Obama*
- *Why Not??*
- *Can't want to…maybe.*

What we will learn today…

- *There are some key terms to keep in mind:*
  - *Intent of the law*
  - *Unintended consequences*
  - *Time and Money*
  - *Any IP Address vulnerable*
  - *Creation to destruction*
  - *Intrusion upon seclusion*
  - *Opt Out vs Opt In (Safe Harbor)*
  - *Analog vs Digital (Data Gridlock)*
  - *MDM vs TDM*

Definitions

One of three major torts is the "intrusion upon seclusion" which imposes liability on "one who intentionally intrudes, physically and otherwise upon the solitude of another or his private affairs or concerns." *FTC*

Definitions

The concept of privacy tort has been a part of the US jurisprudence system since the late 1890s

Opt In refers to an affirmative indication of choice based on the express act of the person giving the consent.

Opt out means the choice can be implied by the failure of the person to object to the use or disclosure.

Privacy?? (1)

Clip 1.mov

- *"wholly Private"*
- *"companies know you"*
- *"surveillance revolution"*
- *"How secure is that DB" – we already know*

"Big Brother if allowed to happen will happen and our job as responsible human beings is to make sure that does not occur"

Privacy?? (2)

Clip 2.mov

- *What is the intent*
- *Unintended consequences*
  - *Case without a cause*
  - *Data collection before Warrant*
- *“benefits of pre-crime surveillance”*
  - *What kind of unintended consequences ??*

Privacy?? (3)

Clip 3.mov

- *"The person whose information is being collected is so out of the loop in this process, and has no rights."*
- *"…secretly they could be using it for something else"*

Privacy?? (4)

Clip 4.mov

- *"I don't have anything to hide"*
- *"I don't use it in a way that can be tracked."*
- *…technology ends up getting used in a way that is exposed and track-able that has not been anticipated."*

Privacy?? (5)

Clip 5.mov

- *Tracking employees:*
  - *Routes*
  - *Speed*
  - *Time in location*
  - *Lunch??*
  - *Restroom breaks??*
- *"If I thought it was a privacy issue, I might have."*
- *"But its not a privacy issue" ????*
- *Would he think it was?*

Privacy?? (6)

Clip 6.mov

- ***With GPS off – Cell phones still tracked and recorded.***
- ***"in public – no expectation of privacy"***

Privacy?? (7)

Clip 7.mov

- *ChoicePoint – 17 Billion records on every US citizen including SSNs.*
- *Sells your data to anyone even for criminal investigations.*
- *CP lost 145,00 records, DVA lost 26.5 million records.*
- *Federal privacy act of 1974 limits government from compiling files on individual Americans. Really??*
- *"My CP report contains SSNs for all my family members."*
- *…they can use this information for many different purposes.*
- *"there was 'no reason' to think these records did not belong to her."*
- *If adverse decision-# of days to dispute-AFTER the damage done, and the job lost.*

Privacy?? (8)

Clip 8.mov

- *AOL…setting up the system to allow the government (more time) to gain access to more and more of your communications.*
- *Google's growing portfolio of products each designed to extract information from the world…is also extracting information about you.*
- *Google has been excluded from a privacy bill designed to regulate data brokers…(like Google).*

Privacy?? *(9)*

Clip 9.mov

- *Why focus on the negative?*
  - *How do you go about getting a new fingerprint issued?*
  - *How to you manage to change your retina?*
  - *How do you manage to alter your face pattern?*
  - *That's why*

"Big Brother if allowed to happen will happen and our job as responsible human beings is to make sure that does not occur"

Privacy?? *(10)*

Clip10.mov

- *With each advance comes an added threat for the technology to be abused.*
- *Will the technology used today to combat crime be used in the future to clamp down on free speech or political dissent?*
- *As is the case with any powerful technology we have to insist on responsible use.*
- *Not worried – we have so much oversight?? Really?*
- *Its going to be critical over the next ten years to try and establish a balance between individuals privacy rights and the ability of government to get our personal information.* *2006 (1986)*

Information Legal Concerns

- ***Our most current laws governing prohibition on snooping on others in the US is 1986.***
- ***What kind of computers and mobile devices did we have then?***
- ***This has become an issue of Digital vs Analog.*** ***Mailbox, wiretap***
- ***We are arresting the victims and not the criminals.*** ***Bank, bull, body***

What foundation is supporting you?

US

Common Law

Opt Out *(if, who)*

53+ standards

EU

Civil Law

Opt In

One standard

US Legal Cont.

- *Initial statute morphs over time and decisions.*
- *Compliance law morphs as well.*
- *Decisions can change previous decisions all the way until the US Supreme Court rules…*
- *The original law may look nothing like the current law due to all the above.*
- *US only major industrialized nation that does not make false accusers responsible for all court costs and damages.*

Forensics and Data against US

- *Michael Caloyannides*
  - *PHD Elect Eng., Applied Math, Philosophy; CalTech*
- *"Digital evidence is often evidence of nothing"*
- *Federal agents must place the user in the crime*

- *How many of you feel comfortable enough with your security policy to guarantee you can "place the user and only the user with access to the data at the time of the cyber crime."?*

Still sure of your position?

- *No C$ shares*
- *No "administrator" accounts*
- *No shared passwords across departments*
- *No way for anyone to view data on the device in question without user knowing it.*

- *Then you are not placing ONLY the user in control of the data at the time of the crime.*

Mikey continues

- *BEST science used – reversed by DNA*
- *We do not have anything close to a cyber DNA*
- *If we did how do we retry cases when the evidence is destroyed*
- *AF hired contractors to teach FLETC agents how not to destroy evidence.*
- *Federal Law is now making it mandatory for a PI to do the Forensic Evidence Gathering*

Lets review some issues

- *4th amendment, probable cause, court order*
  - *Traffic stop*
  - *Meta data*
  - *San Diego file – opt out?*
  - *Inadmissible evidence?*
  - *Slander vs bad data – Damages?*

Review of the legal issues

- *Congress just narrowly agreed to allow the federal government to require and store all metadata from all phones …*
- *No 4th amendment cause for this*
- *No for cause court order prior (congress)*
- *Government is building a potential future case against you now.*
- *We are arresting the victims and not the criminals*

If in the past cases have been lost due to improperly gathered evidence being inadmissible, (i.e.: without a warrant, probable cause and court order) Why are we allowing evidence to be admitted to cases that was generated before there was even a crime or a case?

Federal Law outside the fourth amendment makes it illegal to perform surveillance on US citizens without proper court orders.

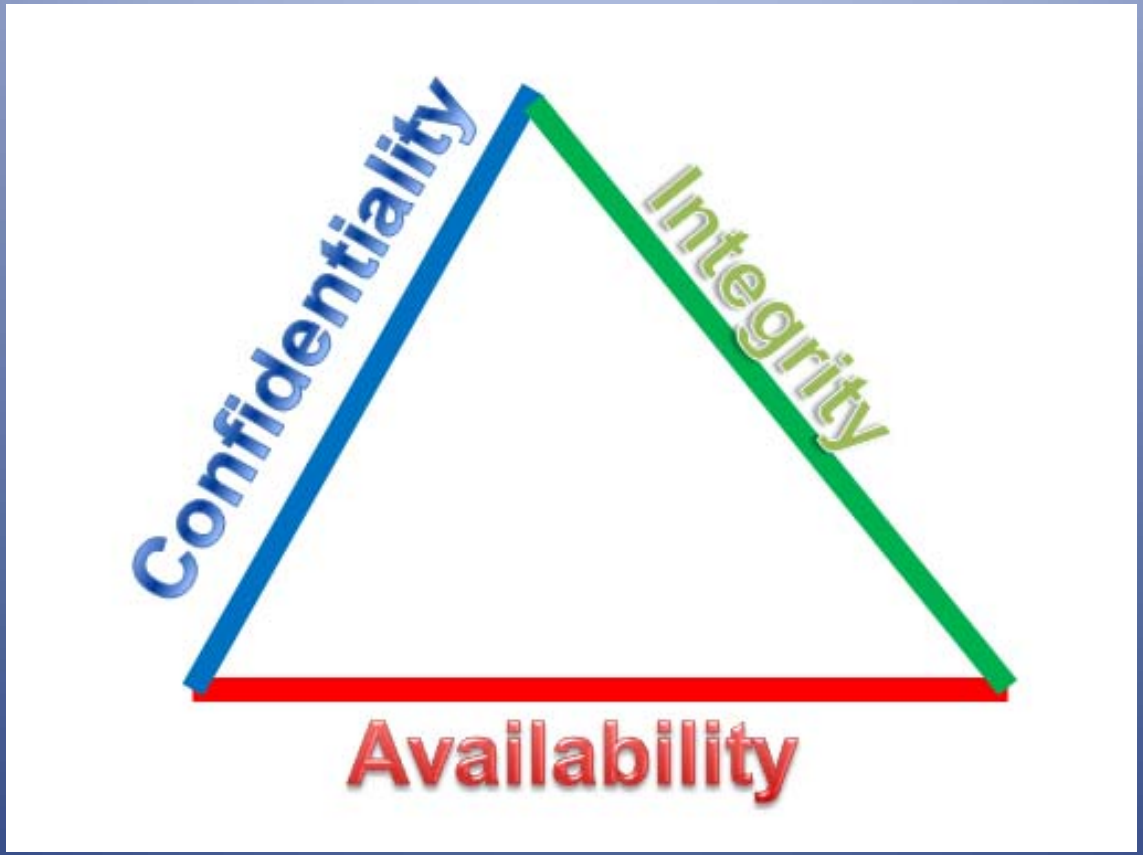
examples

Data Mining on US Citizens is big business, most do not know what is held and stored on them and none have any way to verify their validity.

Now the Federal government has its own data mining facility out west the size of numerous football fields to mine gather and store data on US citizens without court orders, or probable cause.

Is this why we can't want to??

How Does Mobile Figure in?



How Does Mobile Figure in?

Too much exponential availability growth will over run your abilities and budget to maintain the other two legs of the triangle at the same pace.

We are feeding A at the sacrifice of C and I.

Data Check

- ***How many of you can guarantee that any person accessing your data with their BYOD can not print it, save it, post it, move it to the cloud, email it, or screen shot it while on their screen?***
- ***Will your system work on over 6000 different HW/OS combinations?***
- ***If not you have lost control of your data.***

MDM

- *Access control – where*
- *Device control – where – how – 6000 variations.*
- *Data destruction – to DoD standards*
- *SSL secure?*
- *Devices decommissioned properly?*

“The FTC issued a warning to mobile device hardware makers that their devices must be designed and built to a ‘reasonable’ level of security” *CSO magazine online*

“MDM and MAM technologies are incremental. Perhaps they buy the market 18 months of some additional security, but the cat and mouse fight remains.” *Vikram Phatak, CEO NSS Labs*

Cloud

- *Provider s lose data – who pays?*
- *Data retention/holds – dynamic/static*
- *Data Recovery – forensic results*
- *Dynamic Recovery order – forced breech?*
- *Recovery Order to Cloud – Not you?*

“you can delegate tasks and processes but not responsibility.” *USAF - DoD*

Whether it's accessing a SaaS application from your desktop, or a consumer cloud storage provider from your smartphone, the goal, and the challenge, is the same: get my users access to the data they need, and keep everyone else out. Everything else is window dressing.

We can't afford to make the mistake of focusing on one element at the cost of the others. Devices, services, mobility – are simply the details; the real challenge is keeping data available and secure.

- Geoff Web ***11/16/12***

TAKE NOTE

"The line between what is unethical and what is illegal is sometimes blurry and unpredictable. If a company seeks to scrape by doing the minimum the law requires, the odds are fairly high that it will fail in this goal. Those who aim for the bottom tend to miss their low target and eventually break the law." *(Murphy, Joseph E., Joshua H. Leet, and Joseph E. Murphy. Building a Career in Compliance and Ethics)*

How Do We Survive

- *Privacy rule…how would you react if someone imposed your rules on you?*
- *Are we trying to legislate morality?*
- *Are we regulating & restricting productivity?*
- *Are we ready for the legal ramifications?*
- *Are our staff fully trained to be investigators?*
- *Do we want to manage and defend more than we have too?*

Court - Lessons

- *Improper searching for discoverable data could put you in court to defend your processes.*
- *Don't let Law enforcement convince you to act on their behalf without the protection of being a deputized agent.*
- *Know the law…all of it.*
- *Make sure your policies are defendable.*
- *Make sure your policy is written … not practice.*
- *Focus on your need to protect your data, not devices.*

- ***What we do now will determine IF we have ANY privacy in our futures Big Brother Big Business CNBC 2006***
- ***That was stated in 2006 we have three years left and little privacy or security***

So how do we survive in this mess??

Securing the Future?

- ***<u>Education</u> will need to lead in developing new technology for the following issues:***
  - ***A new secure protocol that will leave a users logical DNA on every transaction. (no TCP/IP)***
  - ***Michael Caloyannides, DNA won't free anyone now.***
  - ***FLETC training agent how not to destroy evidence.***
  - ***Protect privacy and internet as securely as we currently protect snail mail and wiretapping.***
  - ***Prosecute on the logical DNA***
  - ***What about those cases lost in the system forever?***
  - ***GPS for data compliance***

Securing the data

- *Treat all devices as dirty…every time.*
- *Allow view only access to our data from outside our internal network*
- *Overwrite all memory used when connection dropped*
- *Do not manage devices – control data.*
- *Ensure no loss of control on any access option.*

Securing the bottom line

- *No data left on mobile devices*
- *No critical data on the end of an IP address*
- *NEW protocols needed for secure internet.*
- *Digital DNA*
- *Aggressive prosecution*
- *Insist on non – repudiation*
- *Be over protective when needed.*
- *Once data is out there it will not come back!*

"Be careful Out There"

Questions??????????

Gordon Merrill, MSIA, CISSP

Merrill.IA@gmail.com

423-280-2892

For more on this subject contact me to gain a For More Info resource page