

Technology myths shattered: Privacy in the digital age

GPEN Pacific Teleconference
7 May 2014

Stephen Wilson
Lockstep Group

LOCKSTEP

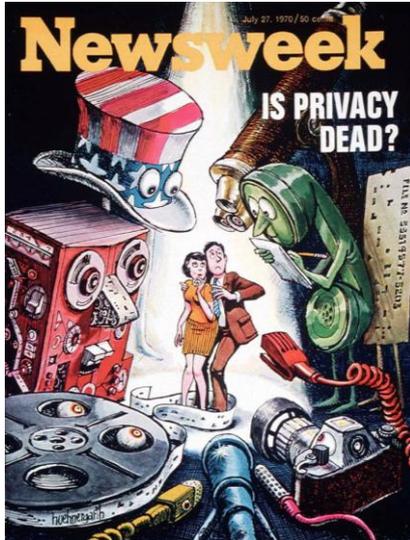


Agenda



- The intersection between privacy and big data – is the law really so far behind?
- How can privacy enforcement staff better engage with IT to encourage proactive privacy compliance?

Impressions, slogans & mixed messages



- “Privacy is dead”
- “Privacy is not a technology issue”
- “Privacy is good for business”
- Quality was good for business
- Security was good for business
- Privacy “is about control”
- But increasingly control is moot
- Technology neutrality (or timidity)
- Focus on anonymity
(PETs, Tor, encryption, Bitcoin)
- Category error in the PII “trade”

Category error



Google "trade privacy for"

Web Images Maps Shopping Videos More Search tools

Page 4 of about 382,000 results (0.21 seconds)

[Will drivers trade privacy for discounts? - Red Tape](#)
redtape.nbcnews.com/_.../6345832-will-drivers-trade-privacy-for-dis...
Sep 9, 2008 – Of all the things that seem unfair about auto insurance, this is perhaps the worst: Infrequent drivers who log less than 5000 miles a year, are ...

[Technologies trade privacy for greater security](#)
www.eetimes.com > News and Analysis
Sep 21, 2001 – PARK RIDGE, Ill. — As the U.S. government raises the specter of a society bounded by electronic-monitoring techniques, security experts are ...

[Schneier on Security: Trading Privacy for Convenience](#)
www.schneier.com/blog/archives/2006/05/trading_privacy.html
May 16, 2006 – While privacy remains a major concern for people around the world, a majority of consumers would share personal data if they knew the ...

[Infosys CEO: People Trade Privacy for Tech Benefits | PCWorld](#)
www.pcworld.com/article/206103/article.html
Sep 23, 2010 – People are willing to change their definition of privacy if they benefit from



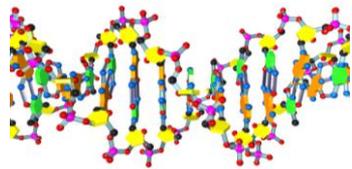
Case studies and Lessons



- Google Streetview Wi-Fi collection
→ being public doesn't negate privacy



- Facebook biometric tag suggestions
→ indirectly collected PII still protected
→ Privacy Law has teeth



- Target pregnancy detector
→ Big Data is an indirect collection
→ special risks synthesising health info

- DNA "hacking"
→ if unlawful in EU, unethical in US?

Common ground and new messages



- The Need to Know Principle
- The Principle of Least Privilege
“A user of program must be able to access only the information and resources necessary for its legitimate purpose”
- Privacy is a state, not a thing
- Privacy is not the same as secrecy
- Privacy is never perfect
- Privacy does not require anonymity
- The “genie” is not “out the of bottle”



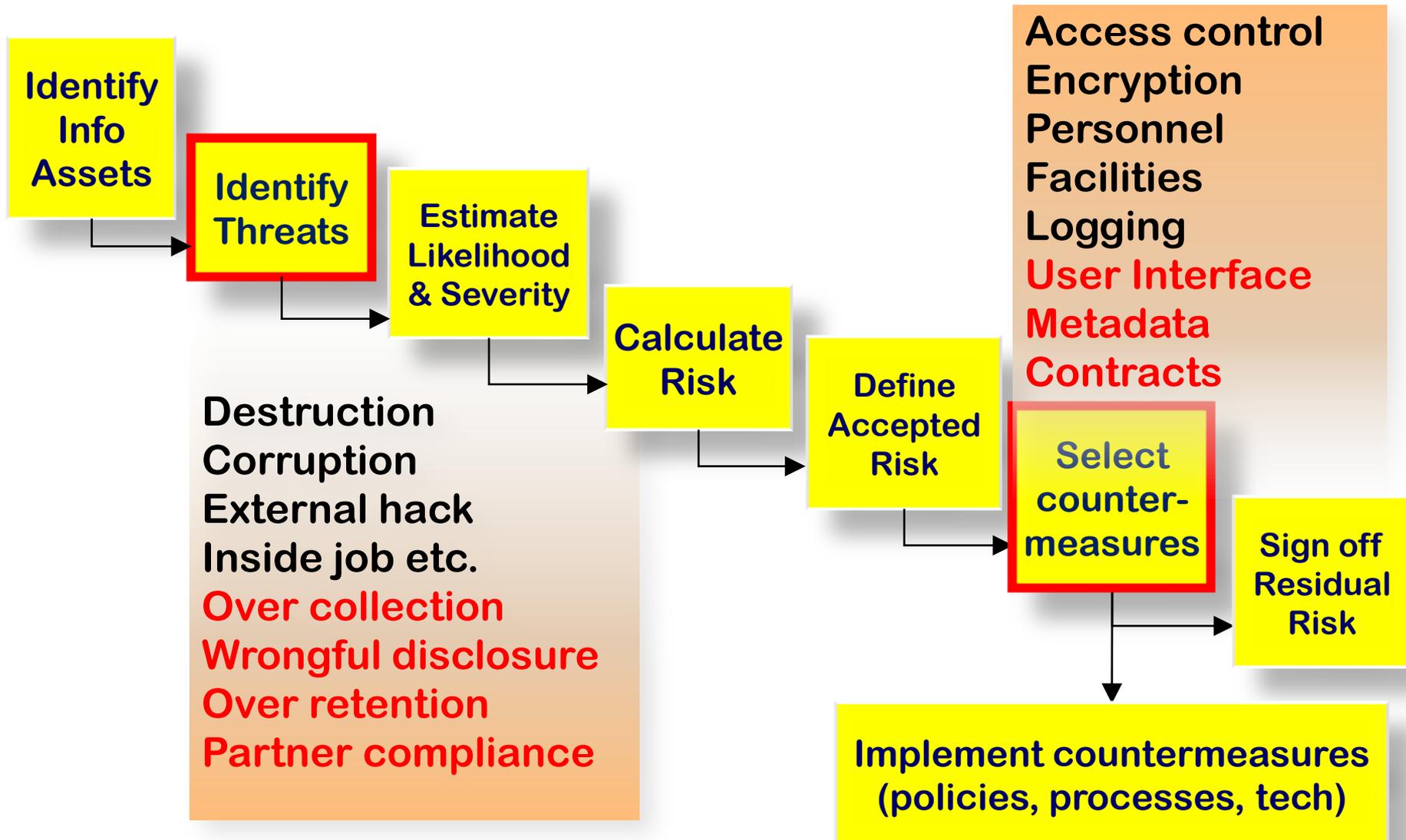
New hybrid approaches to engineer privacy



- Acknowledge the privacy tensions
- Treat privacy as an information asset
- Security = “C.I.A.”; add privacy attributes
- Extended Security Threat & Risk Analysis
- Treat identification as a *risk*
- Safeguard identifiable information *before* it’s actually identified

- “Privacy Engineering”
- Beware of over-collecting (e.g. logs, forms)
- Limit re-use (database schemas, metadata)
- Beware of unintended consequences

Hybrid Privacy Threat & Risk Assessment



Conclusions



Data Privacy is ...

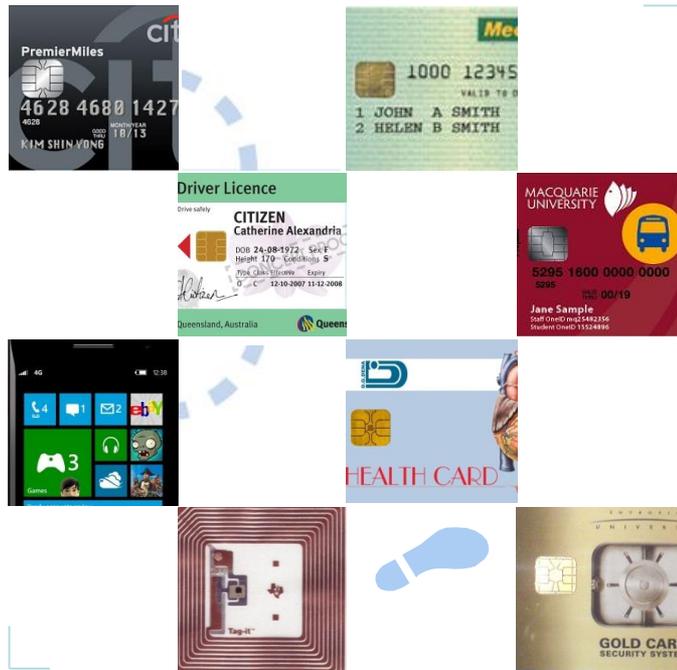
- Not a thing but a state
- More about what you *don't* do
- Not much about security
- Not at all about secrecy
(few really want anonymity)
- Never perfect
- At odds with many IT requirements
- Reducible in system design
- Alive and kicking.



Further reading

- *Not too late for privacy*
<http://lockstep.com.au/blog/2012/10/29/not-too-late-for-privacy>
- *The beginning of privacy*
<http://lockstep.com.au/blog/2013/02/12/the-beginning-of-privacy>
- *“Big Privacy” Rises to the Challenges of Big Data*
constellationr.com/research/big-privacy-rises-challenges-big-data
- *Facebook suspends photo tag tool in Europe* BBC 21 Sep 2012
<http://www.bbc.co.uk/news/technology-19675172>
- *DNA hacking, MIT*
<http://wi.mit.edu/news/archive/2013/scientists-expose-new-vulnerabilities-security-personal-genetic-information>
- *Harvard Law School Petrie-Flom Centre*
Online Symposium on the Law, Ethics & Science of Re-identification
blogs.law.harvard.edu/billofhealth/category/re-identification-symposium

Discussion



swilson@lockstep.com.au
<http://lockstep.com.au/about/privacy>

LOCKSTEP

