beyond security and privacy: trust and the value of data

august 18, 2015, arlington

2015 nsf cybersecurity summit for large facilities and cyberinfrastructure
if your shop assistant was an app ...
(hidden camera)

NOTES

“you have zero privacy anyway. get over it.”

(A) scott mcnealy

(B) COVER OF THE 30 JANUARY 2015 SPECIAL ISSUE OF SCIENCE MAGAZINE TITLED "THE END OF PRIVACY"

NOTES
(A) Sun Microsystems logo.
partial privacy timeline

- 1789: US constitution
- 1890: Brandeis 'right to be let alone'
- 1948: UN declaration of human rights
- 1968: Privacy rulings by SCOTUS
- 60s-70s: Privacy rulings by SCOTUS
- 1972: Privacy added to California constitution as inalienable right
- 1974: Privacy act
- 1977: SCOTUS privacy commission report

NOTES

• Based on a timeline developed by Sol Bermann, Privacy Officer, IT Policy, Compliance, Enterprise Continuity Strategist, at the University of Michigan.
NOTES

(C) Sun Microsystems logo.

what is privacy?
what is privacy?

1. hipaa notice at your doctor’s office?
2. target, neiman marcus, anthem, etc. breaches?
3. annual credit card marketing opt-out mailing?
4. snowden/nsa/government surveillance?
5. facebook/google/uber data mining?
6. the ubiquitous internet “i agree” button?
7. tsa body scanning?
8. a nuisance?
9. other?
Cartoon showing a couple inside a house labeled ‘privacy’ that is being torn down by workmen, while other workmen build a fence around the lot labeled ‘security’.

NOTES

Beyond Security and Privacy: Trust and the Value of Data
2015 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure

information security officer

privacy officer

information security
protects all information

IT security
protects technical infrastructure

information about individuals (e.g., student/patient records; SSNs)

confidential information (e.g., intellectual property, security info)

information

infrastructure (e.g., computers and networks)

information privacy
protects information about individuals
Information security and information privacy tend to complement one another.

- Information security officer protects all information.

- Privacy officer protects information about individuals (e.g., student/patient records; SSNs).

- Compliance includes:
  - Privacy rules – HIPAA, FERPA, …
  - State breach notification laws
  - Open records laws (state, FOIA)

- Fair information practices principles:
  - Notice/awareness, choice/consent,
  - Access/participation, integrity/security,
  - Enforcement/redress

- Dataset techniques:
  - De-identification, anonymization
  - Cell sizes
  - Constraints on use v. collection

Notes:
- Information security and information privacy tend to complement one another.
NOTES

- It's not just security v. privacy, it can be privacy v. privacy
- In some sense, the privacy officer is the people's advocate
information security officer

privacy officer

individuals

- confidential information (e.g., intellectual property, security info)
- information about individuals (e.g., student/patient records; SSNs)

information

infrastructure (e.g., computers and networks)

information security protects all information

IT security protects technical infrastructure

autonomy privacy covers individuals from observation

privacy protects information about individuals

NOTES

• Based on the diagram from the report below. See <http://ucop.edu/privacy-initiative> for further information.
NOTES

netsage

an open privacy-aware network measurement, analysis, and visualization service designed to address the needs of today’s international networks

NOTES

in recent years a number of universities including UCLA have received public records requests seeking disclosure of faculty members’ scholarly communications. the potential chilling effect of these requests has raised new questions about academic freedom and its intersection with public institutions’ legal obligations to conduct business transparently.

— UCLA chancellor gene block

NOTES

but if someone wanted to do this at UCLA, who would they ask? how would the decision be made?

NOTES

such student analytics is not considered to be human subjects research

NOTES

"chief human resources officer ibm watson"
big data privacy hazards
indiscriminate collection of data
data generation
predictive analysis
indefinite storage
data breaches

volunteered data
observed data
inferred data

descriptive – summarize what happened
predictive – forecast what may happen in the future
prescriptive – recommend one or more courses of action

NOTES
• Based on material from Doron Rotman, KPMG
fipps is meaningless!?

q: how would the NSA write a meaningful privacy notice?
q: how would facebook write a useful privacy notice?
NOTES

Beyond Security and Privacy: Trust and the Value of Data
2015 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure
balancing a constellation of obligations, values and consequences

NOTES

• From a 2010 presentation to the University of California President’s Privacy and Information Security Initiative Steering Committee.
these scenarios are challenging because:
1. we have discretion
2. we are often weighing values against the concrete
3. once the irb says its not under their purview, there nowhere else to turn
“mission first” governance
operationally: contracts, good stewardship, transparency, predictability, …

NOTES

working with your privacy officer
commonalities

• data classification
• reviews of contracts and agreements (cloud + international)
• community awareness
• need for “[privacy, security, accessibility] by design”
NOTES

• Regardless of whether you agree or disagree / like or dislike, these have served well to catalyze discussion.


Beyond Security and Privacy: Trust and the Value of Data
2015 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure
• the new kid on the block … e.g., incident response

“we should not be building surveillance technology into standards. law enforcement was not supposed to be easy. where it is easy, it’s called a police state.”

— jeff schiller (wired, 1999)

NOTES
• the ‘no’ (wo)man

“WHAT WE SAY TO DOGS” CARTOON BY GARY LARSON IN THE FAR SIDE, SHOWING A MAN TALKING TO HIS DOG AND THE DOG ONLY HEARING HER NAME.

NOTES

BREACHES OF PERSONAL INFORMATION
- Campus response policy and protocol
- Keynote: Surviving a privacy breach

PROTECTING DATA
- Data classification and other policy
- Data in the cloud
- Concrete suggestions for better awareness

PROTECTING DEVICES AND INFRASTRUCTURE
- Keynote: Surviving a high-profile burglary
- Cybersecurity insurance claims and eligibility
- Campus backbone network protections
- Campuswide initiatives and policy

BALANCING PRIVACY INTERESTS
- Privacy expectations, policy requirements, and the law
- HR and IT procedures for new and separating staff

This seminar is organized by the Office of the UCLA Chief Privacy Officer, supported by the Office of Information Technology, and sponsored by the Office of Insurance and Risk Management.
DATA PROTECTION SEMINAR
February 10, 2015 | Faculty Center, California Room | 8 AM – 12 noon

Campus Counsel
Campus Human Resources
Campus Backbone Networking
Chief Compliance Officer, Health Sciences
Chief Information Security Officer
Insurance and Risk Management
IT Policy
Library
Procurement
UCLA Chief Privacy Officer

This seminar is organized by the Office of the UCLA Chief Privacy Officer, supported by the Office of Information Technology, and sponsored by the Office of Insurance and Risk Management.
the creepiness test

when embarking on something new, ask yourself: will someone be creeped out if they knew i was doing this?

the test isn’t so much about whether the feeling is based on reality, but on avoiding erosion of trust.

NOTES


NOTES

Additional Notes

1. The concept (value) of academic freedom
   • I often show an architectural drawing and real-life building of Jeremy Bentham’s panopticon to illustrate the chilling effect of surveillance.
   • Sarah Lewis spoke at the 2015 IAPP Global Privacy Summit of the need for private spaces in which to fail without the judging eyes of the public or peers. Also see.

2. Recommendations about a governance structure and principles that can be used to balance UCLA’s many values and obligations when considering the appropriate use of data about its community will be forthcoming from the Data Governance Task Force, jointly charged by the Academic Senate and the Administration.

3. A two-minute video by vendor Silent Circle demonstrating what apps can do with your personal info can be found at.

NOTES