kent wada
director, strategic IT policy and chief privacy officer

an institutional framework for privacy in higher education

educause annual conference
anaheim, october 16, 2013
['how to order a pizza in 2015’ video]
pizza palace was ‘wired into the system’ and can now build a profile of you

what you’re reading
your health
your social security number
your credit card numbers
your finances
where you travel
where you are
your purchases
your employment history
your driver’s license number
your personal stats
your contact info
our institutions don’t just have access to this data, we actually have this data

library circulation records
patient records
social security number
credit card numbers
background checks, financial aid, investments
tavel records
ip address logs, ‘find my iphone’
bookstore, faculty club
academic and staff personnel records
driver’s license number
birthday lunches, student athlete stats
student records
and so much more

- library circulation records
- patient records
- social security number
- credit card numbers
- background checks, financial aid, investments
- travel records
- ip address logs, ‘find my iphone’
- bookstore, faculty club
- academic and staff personnel records
- driver’s license number
- birthday lunches, student athlete stats
- student records
- human subjects research data
- animal researchers
- email, text pages, voicemails
- disabilities disclosures
- calendars
- law enforcement records
- firewall connection logs
- donor records
we’ve only begun to correlate across our information sources.

university officials could potentially mine data from their students and analyze them, since the data are already under their control. the analysis could then be screened to predict behavior to identify when a student’s online activities tend to indicate a threat to the campus.

mining student data could save lives
the chronicle, 10/2/2011

[advertisement from target about ‘target baby alerts’]

Image can be found at http://targetimages.bfio.com/Everest/tgt/2012/12_28/5D_baby/comp/comp3_5D_baby_targetBaby.jpg, which is referenced from the page http://www.mailboxr.com/2012/12/28/target-new-baby-must-haves-organization-sale/.
linked to your target guest id

if you use a credit card or coupon
if you fill out a survey
if you get a refund
if you call the customer help line
if you open an e-mail
if you visit the web site
your age
married?
have kids?
which part of town you live in
time to drive to store?
estimated salary
moved recently?
credit cards are in your wallet?
what web sites you visit
data target can purchase

ethnicity
job history
the magazines you read
declared bankruptcy?
gotten divorced?
year you bought your house
where you went to college
topics you talk about online
brand preferences
political leanings
reading habits
charitable giving
number of cars you own

think
• surveillance, “big brother”
• the monitoring of behavior
• big data, data mining, profiling

related to
• first amendment: freedom of association
• anonymity

civil liberty (people)

information stewardship (about people)

think
• ferpa, hipaa, glba, irbs
• pci-dss
• ftc red flags rule
• state breach notification laws
• state open records laws
• e-discovery, subpoenas, search warrants, nsls

related to
• compliance
• ethics
<table>
<thead>
<tr>
<th>autonomy (people)</th>
<th>privacy</th>
<th>information (about people)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• surveillance, “big brother”</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• the monitoring of behavior</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• big data, data mining, profiling</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• first amendment: freedom of association</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• anonymity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• ferpa, hipaa, glba, irbs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• pci-dss</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• ftc red flags rule</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• state breach notification laws</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• state open records laws</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• e-discovery, subpoenas, search warrants, nsis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• compliance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• ethics</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
autonomy privacy

an individual’s ability to conduct activities without concern of or actual observation

the traditional realm of the individual (consumer)

information privacy

the appropriate protection, use, and dissemination of information about individuals

the traditional realm of the privacy officer (institution)

The definitions of autonomy and information privacy are from the 2013 report arising out the University of California President’s privacy and information security initiative. Background about this initiative can be found at http://privacyinitiative.universityofcalifornia.edu/.
This diagram is from the 2013 report arising out the University of California President’s privacy and information security initiative. Background about this initiative can be found at http://privacyinitiative.universityofcalifornia.edu/.
individuals

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

autonomy privacy covers individuals from observation

information privacy protects information about individuals

nb. it’s often autonomy privacy v. information privacy not privacy v. security!
autonomy privacy

an individual’s ability to conduct activities without concern of or actual observation

the traditional realm of the individual (consumer)

information privacy

the appropriate protection, use, and dissemination of information about individuals

the traditional realm of the privacy officer (institution)
<table>
<thead>
<tr>
<th>autonomy privacy</th>
<th>information privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>an individual’s ability to conduct activities without concern of or actual observation</td>
<td>the appropriate protection, use, and dissemination of information about individuals</td>
</tr>
</tbody>
</table>

the privacy officer

driving towards a unified privacy approach that gives equal consideration to autonomy privacy and the academy
[architectural design of the panopticon by jeremy bentham, 1748-1832]

The photo can be found at http://newsjunkiepost.com/2011/05/02/privacy-freedom-and-the-all-seeing-eye-the-panopticon/panopticon_black-2/.
[photo of a real-life panopticon]

academic and intellectual freedom are values of the academy that help further the mission of the university. these freedoms are most vibrant where individuals have autonomy: where their inquiry is free because it is given adequate space for experimentation and their ability to speak and participate in discourse within the academy is possible without intimidation. privacy is the condition that makes these values possible.

ucla statement on privacy and data protection
UCLA students can now protect their laptops with FrontDoorSoftware Loss & Recovery

FREE!

Installations include laptop registration, new talk feature, and 4 years of software tracking service. Protect your laptop, information, music, emails and pictures for free today.

INSTALL NOW!
www.frontdoorsoftware.com/UCLA

Front Door Software is available to the UCLA community (http://www.frontdoorsoftware.com/ucla/) to help address the problem of laptop theft (http://map.ais.ucla.edu/go/1005245). See flyer (http://www.ucpd.ucla.edu/2011/FrontDoorSoftware.pdf) and Daily Bruin article (http://dailybruin.com/2012/01/24/ucla_offers_free_laptop_theft_protection_and_tracking_software/) for more information. Use on personally owned laptops is at the discretion of each individual. For University laptops, care must be exercised in the use of this or similar software to ensure tracking is appropriately used. Guidance is being developed through the UCLA Board on Privacy and Data Protection.
photo of a lower merion school district student in his bedroom
one of ~56,000 photos taken by school laptop antitheft software

[trailer for the documentary film “terms and conditions may apply”]
institutional expectations

versus

the expectations of individuals (e.g., byod)
partnering with external vendors (e.g., google, dropbox)
risk of government security activity
proliferating external obligations and consequences
the expectations of individuals (e.g., byod)

partnering with external vendors (e.g., google, dropbox)

proliferating external obligations and consequences

risk of government security activity

the institution needs to balance ...

increased demand for data sharing

research and innovation

technology

information security

operational efficiency

transparency as a public entity
privacy is always a balancing act
with other obligations, values, and consequences of the institution

how?
an institutional approach for balancing privacy with other values and obligations

makes privacy “visible”
privacy program point

+ definitions

statement of privacy values
privacy principles
privacy framework
balancing process

privacy official
privacy governance

strategic direction setting
privacy balancing

This framework is being proposed by the 2013 report arising out the University of California President’s privacy and information security initiative. Background about this initiative can be found at http://privacyinitiative.universityofcalifornia.edu/.
privacy framework + “mission first” analysis
<table>
<thead>
<tr>
<th>operationally critical</th>
<th>institutionally strategic</th>
</tr>
</thead>
<tbody>
<tr>
<td>prevents the mission from</td>
<td>enables the missions of</td>
</tr>
<tr>
<td>being disabled</td>
<td>teaching and research</td>
</tr>
<tr>
<td>ethics and compliance</td>
<td>academic freedom</td>
</tr>
<tr>
<td>information security</td>
<td>autonomy privacy</td>
</tr>
<tr>
<td>information privacy</td>
<td></td>
</tr>
</tbody>
</table>

both are important, but for completely different reasons

the analysis is directly linked to an institution’s mission (“mission first”)
consider the missions of, and resulting balance analyses for:

- individuals
- google
- dropbox
- government
parting thoughts
[“if you have something you don’t want anyone to know, maybe you shouldn’t be doing it in the first place”]

googles chief executive eric schmidt

From a 2009 interview with CNBC’s Maria Bartiromo.
then what do you have to fear?


“'I've got nothing to hide' and other misunderstandings of privacy.” ssrn.com/abstract=998565.
[clip of 2009 interview with former nsa analyst russell tice on nbc’s countdown with keith olbermann]
you have no privacy anyway.

get over it.*

*scott mcnealy, co-founder, sun microsystems. 1999.
kent wada
director, strategic IT policy and chief privacy officer

an institutional framework for privacy in higher education

educause annual conference
anaheim, october 16, 2013
[the following slides give additional material not included in the presentation]
the right to be let alone . . . the right most valued by civilized men

u.s. supreme court justice louis brandeis
harvard law review, 1890
down the hall in the billing department, a clerk uses a lunch break to scan the web for information on abuse victims. The information retrieved also flashes onto a screen in the boss’s office, revealing a secret the employee never told anyone.

“Zuckerberg decides that he should use social influence within Facebook to increase organ donor registrations. Users are given an opportunity to click a box on their timeline pages to signal that they are registered donors, which triggers a notification to their friends. The new feature starts a cascade of social pressure, and organ donor enrollment increases by a factor of 23 across 44 states.”

the statement of privacy values declares privacy—of both autonomy and information—as an important value of the university, as this is not explicitly done elsewhere; and clarifies that privacy is one of many values and obligations of the university.
The privacy principles are derived from the statement of privacy values and established privacy principles, and are intended to guide policies and practice.

E.g., notice and transparency. Conceptually simple, astonishingly hard to implement.
the privacy balancing process is intended as a tool to guide policy development and decision-making when competing privacy interests, university values, or obligations exist and for which no statutory provision, common law, or university policy is directly applicable.
equal faculty and administration
one undergraduate and one graduate student

reports to the executive vice chancellor and provost, with links to the academic senate and the campus ethics, risk, and compliance committee

guides the privacy official

building a unified privacy approach that gives equal consideration to autonomy privacy and the academy

many existing functional offices with compliance responsibility