The Need for Transparency in Privacy Statements & Practices

Annie I. Antón
North Carolina State University

Security and Liberty Forum
University of North Carolina
Chapel Hill, NC

April 14, 2007
Context

- We’ve been studying privacy policy & healthcare privacy for 8 years

- Much of what we do in today’s society involves information exchange and surveillance
  - e.g. government, commerce, healthcare

- For people to be comfortable and willing to take full advantage of IT services we need to:
  - Safeguard their privacy
  - Let them understand we’re safeguarding their privacy and identity
Outline

- Why do we care about transparency?
- Why do we care about privacy?
- Investigation framework
  - Analyzing privacy values vs. practices
  - Readability of privacy policies
  - User perception vs. comprehension of policies
  - To whom do we turn if we have questions?
- Recommendations
Why do we care about transparency?

- Privacy policies are the standard to which organizations are held accountable.

- Transparency increases accountability.

- “Transparency is a clear, complete and readily available notice on an organization’s privacy policies and practices.” [www.nymity.com]

- “Experts agree that good privacy begins with effective transparency. Transparency requires privacy notices that are easy to understand, facilitate comparison, and are actionable. Privacy notices must also comply with legal requirements ....” [www.hunton.com]
Medical Privacy in Particular

- Many medical conditions have some stigma associated with them

- Willingness to pay for treatment “out of pocket” or avoid life-saving treatment to keep information private

- Privacy concerns sometimes cause patients to withhold information that can prevent them from receiving the right kind of treatment

- In the U.S., HIPAA requires health care providers to secure medical records, etc.
“Your DNA doesn’t match your credit history.”
Concerns About Healthcare Privacy in the U.S.

Government Report Finds Health Care Privacy Breaches Rampant

Agencies and contractors that experienced privacy breaches collectively have access to medical data for more than 100 million Americans.

By Thomas Claburn
InformationWeek
Sep 5, 2006 07:00 PM

Over 40% of federal health insurance contractors and state Medicaid agencies reported experiencing a privacy breach involving personal health information in the past two years, according to a Government Accounting Office (GAO) report released on Tuesday.
Consider ...

- Data mining for anti-terrorism
- Airline passenger name record sharing w/ DHS
- ChoicePoint, Bank of America and other record thefts

All of these have been perceived as violations of privacy. And all have provoked public dismay and protest.
An example of when things go wrong ...
jetBlue Analysis (Feb ‘04)

World of Information

Commercial Players

- Experian
- ACXIOM
- Equifax
- DMA
- ChoicePoint
- TransUnion
- LexisNexis
Information Control

Data Aggregators’ Data Quality & Responsiveness

- Study examined the quality of data provided by ChoicePoint and Acxiom

- 100% of the reports given out by ChoicePoint had at least one error in them.

- Error rates for basic biographical data (including information people had to submit in order to receive their reports) fared almost as badly:
  - Acxiom had an error rate of 67%
  - ChoicePoint had an error rate of 73%.

*The majority of participants had at least one significant error in their reported biographical data from each data broker.*

http://www.privacyactivism.org/docs/DataAggregatorsStudy.html
"The computer links me to an international database for who's 'Naughty and Nice'!"
Transparency …

- Transparency increases accountability …
Online, how do you assure the public?
“Congratulations, Dave! I don't think I've read a more beautifully evasive and subtly misleading public statement in all my years in government.”
In particular, how …

- do we assure that
  - policy complies with law?
  - system requirements comply with policy?
  - info. handling adheres to policy and system requirements?

- can policy be associated with data to ensure policies survive system boundaries?

- best do we support different social and legal definitions of privacy?
Policy Content Analysis Using Antón & Earp Taxonomy …

[Requirements Engineering Journal, 2004]

- **Privacy Protection Goals**
  - Access/Participation
  - Choice/Consent
  - Enforcement/Redress
  - Integrity/Security
  - Notice/Awareness

- **Privacy Vulnerabilities**
  - Aggregation of Information
  - Collection of Information
  - Monitoring of Information
  - Personalization
  - Solicitation
  - Storage of Information
  - Transfer of Information
How does this relate to what users think?

What aspects of privacy are most important to on-line consumers?

Let’s also ask:

Are consumers worried about the correct things?

Do institutions understand consumers’ privacy concerns?
Privacy Survey Instrument

Privacy Values Baseline Reveals Misalignment


- Data was collected from 1005 Internet users in 2002 to establish a privacy values baseline for correlation with our privacy protection goals and privacy vulnerabilities taxonomy.

- Consumers are most concerned with (in order):
  - information transfer
  - notice/awareness
  - information storage

- Privacy policies emphasize (in order)
  - data integrity/security
  - information collection, and
  - user choice/consent

Results Available:
http://theprivacyplace.org/
Are privacy statements readable?
Readability Impact

- Only 52.1% of general population has obtained at least 2 years of college

- Healthcare Industry
  - 24 online privacy documents at 9 healthcare websites
  - Flesch readability level = 14.2 (2 years of college)

- Financial Industry
  - 40 online privacy documents at 9 financial websites
  - Flesch readability range = 10.42 – 18.72
  - Flesch readability level = 14.1 (2 years of college)

- Difficult policies are time consuming to read
Missing the intent of GLBA’s clarity requirement

- The stark reality:
  - 8 require equivalent of a high school education or less
  - 13 require equivalent of some college education
  - 12 require 14-16 years of schooling
  - 1/6 require the equivalent of a postgraduate education (> 16 years).
  - 2/3 institutions had at least one policy document requiring the equivalent of a postgraduate education

- A full understanding of what 2/3 of these organizations are promising is only available to <15% of the adult Internet population
“Experts agree that good privacy begins with effective transparency. Transparency requires privacy notices that are easy to understand, facilitate comparison, and are actionable. Privacy notices must also comply with legal requirements ....”

[www.hunton.com]
User perception vs. comprehension of policies...
2005 Privacy Policy Experiment

- Investigate user comprehension and perception of privacy policy expressions
- Theoretical framework based on the Privacy Requirements Taxonomy

- Gauge user perception of various alternatives to natural language privacy policies
- Measure user comprehension of the alternatives
- Compare user perception with user comprehension in order to determine whether they are in alignment with one another
Experimental Design: Blocking Factors

- Drugstore.com
  - More vulnerable for consumers

- Healthcentral.com
  - Control

- Novartis.com
  - More protective for consumers
Experimental Design:
Four variants (treatments)

- Original natural language policy
- List of privacy goals and privacy vulnerabilities
- Categorical representation based on the taxonomy
- Original natural language policy supplemented with highlighted privacy goals and vulnerabilities
## Experimental Design (n=993)

<table>
<thead>
<tr>
<th></th>
<th>Original NL Policy</th>
<th>Goals &amp; Vulnerabilities</th>
<th>Categorical</th>
<th>G/V &amp; Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>More Vulnerable</td>
<td>76</td>
<td>80</td>
<td>77</td>
<td>93</td>
</tr>
<tr>
<td>Control</td>
<td>86</td>
<td>87</td>
<td>81</td>
<td>83</td>
</tr>
<tr>
<td>More Protective</td>
<td>77</td>
<td>81</td>
<td>83</td>
<td>89</td>
</tr>
</tbody>
</table>
Respondent Demographics
(n=993)

- 41.33% engage in online healthcare research at least once a month
- 31.7% have made a healthcare related purchase online
- 53.95% have beyond a college degree
- 29.74% female
- 66.87% male
“I feel secure sharing my personal info with BrandX after viewing their privacy practices”

<table>
<thead>
<tr>
<th>Policy Variant</th>
<th>Average Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Goals/Vulnerabilities &amp; Original Policy</td>
<td>2.85</td>
</tr>
<tr>
<td>Original Policy</td>
<td>2.72</td>
</tr>
<tr>
<td>Categorical</td>
<td>2.58</td>
</tr>
<tr>
<td>Goals/Vulnerabilities</td>
<td>2.44</td>
</tr>
</tbody>
</table>

Users perceive websites that express privacy policy with G/V highlights to be more secure.
“I believe BrandX will protect my personal information more than other companies”

<table>
<thead>
<tr>
<th>Variant</th>
<th>Average Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Goals/Vulnerabilities &amp; Original Policy</td>
<td>2.80</td>
</tr>
<tr>
<td>Original Policy</td>
<td>2.71</td>
</tr>
<tr>
<td>Categorical</td>
<td>2.60</td>
</tr>
<tr>
<td>Goals/Vulnerabilities</td>
<td>2.60</td>
</tr>
<tr>
<td><strong>Average</strong></td>
<td><strong>2.68</strong></td>
</tr>
</tbody>
</table>

Users perceive websites that express privacy policy with G/V highlights as more protective.
"I believe BrandX will protect my personal information more than other companies"

<table>
<thead>
<tr>
<th>Originating Website</th>
<th>Average Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>HealthCentral (control)</td>
<td>2.74</td>
</tr>
<tr>
<td>Novartis (more protective)</td>
<td>2.73</td>
</tr>
<tr>
<td>Drugstore.com (more vulnerable)</td>
<td>2.57</td>
</tr>
</tbody>
</table>

Users are able to distinguish between most vulnerable website & more protected ones.
“I feel that BrandX’s privacy practices are explained thoroughly in the policy I read”

<table>
<thead>
<tr>
<th>Variant</th>
<th>Average Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Original Policy</td>
<td>3.34</td>
</tr>
<tr>
<td>Goals/Vulnerabilities &amp; Original Policy</td>
<td>3.33</td>
</tr>
<tr>
<td>Categorical</td>
<td>2.88</td>
</tr>
<tr>
<td>Goals/Vulnerabilities</td>
<td>2.77</td>
</tr>
<tr>
<td><strong>Average</strong></td>
<td><strong>3.06</strong></td>
</tr>
</tbody>
</table>

**Most explained:**
- GV & Policy variant
- Drugstore.com

**Least explained:**
- ★ Categorical variant ★
- Novartis.com
“I feel that BrandX’s privacy practices are explained thoroughly in the policy I read”

<table>
<thead>
<tr>
<th>Originating Website</th>
<th>Average Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drugstore.com (more vulnerable)</td>
<td>3.25</td>
</tr>
<tr>
<td>HealthCentral (control)</td>
<td>2.99</td>
</tr>
<tr>
<td>Novartis (more protective)</td>
<td>2.96</td>
</tr>
</tbody>
</table>

Users perceive length as reflecting thoroughness.
“I feel confident in my understanding of what I read of BrandX’s privacy policy”

<table>
<thead>
<tr>
<th>Policy</th>
<th>Average Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>HealthCentral (control)</td>
<td>3.27</td>
</tr>
<tr>
<td>Novartis (more protective)</td>
<td>3.24</td>
</tr>
<tr>
<td>Drugstore.com (more vulnerable)</td>
<td>3.05</td>
</tr>
<tr>
<td><strong>Average</strong></td>
<td><strong>3.19</strong></td>
</tr>
</tbody>
</table>

User confidence in understanding raises interesting questions about perception of thoroughness.
Example Quiz Question

Which statement is TRUE regarding BrandX's information collection practices?

- BrandX collects Personal Health Information (PHI) in order to fill a prescription
- BrandX collects information about your browser type
- BrandX collects information from customer emails sent to their institution
- BrandX collects information from forms filled out on their site
- The policy does not address how information is collected
# Average Comprehension Score

All respondents (p<.0001)

<table>
<thead>
<tr>
<th>Variant</th>
<th>Average</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Categorical</strong></td>
<td><strong>52.14</strong></td>
</tr>
<tr>
<td>Goals/Vulnerabilities</td>
<td>43.82</td>
</tr>
<tr>
<td>Goals/Vulnerabilities &amp; Original Policy</td>
<td>43.27</td>
</tr>
<tr>
<td>Original Policy</td>
<td>35.70</td>
</tr>
<tr>
<td><strong>Average</strong></td>
<td><strong>43.74</strong></td>
</tr>
</tbody>
</table>

User perception and comprehension are misaligned.
# Average Comprehension Score

(only respondents who read the entire policy)

<table>
<thead>
<tr>
<th>Variant</th>
<th>Average</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Categorical</strong></td>
<td>65.67</td>
</tr>
<tr>
<td><strong>Goals/Vulnerabilities</strong></td>
<td>55.46</td>
</tr>
<tr>
<td>Goals/Vulnerabilities &amp; Original Policy</td>
<td>49.38</td>
</tr>
<tr>
<td>Original Policy</td>
<td>40.00</td>
</tr>
<tr>
<td><strong>Average</strong></td>
<td>52.88</td>
</tr>
</tbody>
</table>

User perception and comprehension are misaligned.
“I read the entire set of privacy policies of the website”

- Categories 62%
- Policy 56%
- Goals/Vulnerabilities & Policy 50%
- Goals/Vulnerabilities 44%
Comprehension Summary


- Users comprehend natural language policies the least
- Simply adding goals to natural language policies increased comprehension
- Significant increase in comprehension when goals are categorized
- Scores alarmingly low, despite which variant used
What about demographics?

- No correlation between demographic factors and comprehension/perception exists.

- Exception
  - Respondents age 57 and higher scored lower on comprehension questions
Summary of User Perceptions


- Users believe:
  - they are more secure sharing PII with websites that display NL policies that highlight the goals and vulnerabilities
  - the companies that display NL policies that highlight goals and vulnerabilities will protect their information the most
  - the two NL variants are explained more thoroughly than alternative expressions

- User perception and comprehension are misaligned!!
  - Users feel most secure and protected by natural language policies, but comprehend them the worst
What if we have questions about an organization’s privacy policy?
Objective:
- Contact each airline via the contact provided on their Privacy Policy to specifically ask questions regarding their privacy policy to determine each airline’s preparedness to respond to such inquiries.

Mechanisms:
- Telephone
- Web Forms
- Email
Phone Script

Hello, my name is Annie Antón/Paul Otto. I've read your privacy policy and have a few questions about it, so I'm calling the number that you provided should we have additional questions ...

- With whom specifically does ___________ share customer information?
  - Do you share it with:
    - DHS?
    - TSA?
    - Data Brokers like Axiom & ChoicePoint?
    - Direct Marketers?

- Who are your third parties?
  - What do you get in exchange for this sharing?

- What specific information do you share with these companies?
<table>
<thead>
<tr>
<th>Airline</th>
<th>Original Contact Date</th>
<th>Original Contact Type</th>
<th>Airline Reply to 1st Inquiry Date</th>
<th>Lapsed Time</th>
<th>Response Quality</th>
<th>Response Author</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.S.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AirTran Airways</td>
<td>05/17/10</td>
<td>web form</td>
<td>5/17/10</td>
<td>same day</td>
<td>pending</td>
<td>auto</td>
<td>will reply w/in 72 business hrs; if request is urgent call cust serv: 800.airtran; your email has been forwarded to website development group; someone will respond promptly</td>
</tr>
<tr>
<td></td>
<td>05/17/10</td>
<td>web form</td>
<td>5/17/10</td>
<td>same day</td>
<td>pending</td>
<td>Theda Moody (cust serv</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>team)</td>
<td></td>
</tr>
<tr>
<td>Alaska Airlines</td>
<td>06/09/10</td>
<td>web form</td>
<td>6/9/10</td>
<td>same day</td>
<td>pending</td>
<td>auto</td>
<td>Please allow one business day for an agent to respond to your email.</td>
</tr>
<tr>
<td>American Airlines</td>
<td>05/17/10</td>
<td>web form</td>
<td>5/17/09</td>
<td>same day</td>
<td>pending</td>
<td>Mr. M. Exter (web services)</td>
<td>please view PP; then, if you require additional assistance, contact web services at: 800.222.2377</td>
</tr>
<tr>
<td>ATA</td>
<td>06/09/10</td>
<td>web form</td>
<td>6/9/10</td>
<td>same day</td>
<td>pending</td>
<td>auto</td>
<td></td>
</tr>
<tr>
<td>Continental Airlines</td>
<td>05/17/10</td>
<td>email</td>
<td>5/24/10</td>
<td>7 days</td>
<td>no answer</td>
<td>senior attorney: Abby</td>
<td>please review privacy policy;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Bried (priv. compliance</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>contact)</td>
<td></td>
</tr>
<tr>
<td>Delta Air Lines</td>
<td>05/17/10</td>
<td>email</td>
<td>5/26/10</td>
<td>9 days</td>
<td>no answer</td>
<td>cust. commitment crew</td>
<td>auto reply acknowledged our email; asked for patience due to volume; but</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>member:  Nancy</td>
<td>response may take longer</td>
</tr>
<tr>
<td>JetBlue Airways</td>
<td>05/17/10</td>
<td>email</td>
<td>5/26/10</td>
<td>9 days</td>
<td>no answer</td>
<td>auto</td>
<td>please review privacy policy; if you have questions please email or call; happy to respond, but more efficient if you first read the PP</td>
</tr>
<tr>
<td>Northwest Airlines</td>
<td>06/09/10</td>
<td>web form</td>
<td>6/9/10</td>
<td>same day</td>
<td>pending</td>
<td>auto</td>
<td>We respond to questions about online bookings within 3 hours, 7 days a week, 24 hours a day. All messages are personally read and handled to give you the attention you deserve. I have researched your inquiry. In order to assist you, please call colleagues in Customer care at: 701.420.6282 (also provided mailing address and fax number). Thank you for writing, we appreciate your patience, I trust that this will assist you with y</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Martez Franklin (cust</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>serv)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Southwest Airlines</td>
<td>05/17/10</td>
<td>phone</td>
<td>5/17/10</td>
<td>same day</td>
<td>pending</td>
<td>auto</td>
<td>a member of our customer relations team will personally review your correspondence and respond as soon as possible; due to current volumes, response time is longer than normal given your situation, you can call our cust. Relation team: 877.228.1327</td>
</tr>
<tr>
<td>United Airlines</td>
<td>05/17/10</td>
<td>web form</td>
<td>5/17/10</td>
<td>same day</td>
<td>pending</td>
<td>auto</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Peter Vohra (cust</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>relations)</td>
<td></td>
</tr>
</tbody>
</table>
## Airline Responses to Inquiry #1

<table>
<thead>
<tr>
<th>Airline</th>
<th>Original Contact Date/Type</th>
<th>Airline Reply to 1st Inquiry Date</th>
<th>Lapsed Time</th>
<th>Response Quality</th>
<th>Response Author</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>U.S.</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AirTran Airways</td>
<td>05/17/10 web form</td>
<td>5/17/10 same day (auto)</td>
<td>pending</td>
<td>auto</td>
<td>Theda Moody (cust serv team)</td>
<td>will reply w/in 72 business hrs; if request is urgent call cust serv: 800.airtran; your email has been forwarded to website development group; someone will respond promptly</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5/17/10 same day</td>
<td>pending</td>
<td>auto</td>
<td>Theda Moody (cust serv team)</td>
<td></td>
</tr>
<tr>
<td>Alaska Airlines</td>
<td>06/09/10 web form</td>
<td>6/9/10 same day (auto)</td>
<td>pending</td>
<td>auto</td>
<td></td>
<td>Please allow one business day for an agent to respond to your email.</td>
</tr>
<tr>
<td>American Airlines</td>
<td>05/17/10 web form</td>
<td>5/17/09 same day</td>
<td>pending</td>
<td>Mr. M. Exter (web services)</td>
<td></td>
<td>please view PP; then, if you require additional assistance, contact web services at: 800.222.2377</td>
</tr>
<tr>
<td>ATA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Continental Airlines</td>
<td>05/17/10 email</td>
<td>5/24/10 7 days</td>
<td>no answer</td>
<td>senior attorney: Abby Bried (priv. compliance contact)</td>
<td></td>
<td>please review privacy policy;</td>
</tr>
<tr>
<td>Delta Airlines</td>
<td>05/17/10 web form</td>
<td>5/17/10 same day (auto)</td>
<td>pending</td>
<td>auto</td>
<td></td>
<td>auto reply acknowledged our email; asked for patience due to volume; but response may take longer</td>
</tr>
<tr>
<td>JetBlue Airways</td>
<td>05/17/10 email</td>
<td>5/26/10 9 days</td>
<td>no answer</td>
<td>cust. commitment crew member: Nancy</td>
<td></td>
<td>please review privacy policy; if you have questions please email or call; happy to respond, but more efficient if you first read the PP</td>
</tr>
<tr>
<td>Northwest Airlines</td>
<td>09/09/10 web form</td>
<td>9/3/10 same day (auto)</td>
<td>pending</td>
<td>auto</td>
<td></td>
<td>We respond to questions about online bookings within 8 hours, 7 days a week, 24 hours a day. All messages are personally read and handled to give you the attention you deserve. I have researched your inquiry. In order to assist you, please call colleagues in Customer care at: 701.420.6282 (also provided mailing address and fax number). Thank you for writing, we appreciate your patience, I trust that this will assist you with your situation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6/10/10 1 day referral</td>
<td>referral</td>
<td>Martez Franklin (cust serv)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Southwest Airlines</td>
<td>phone</td>
<td>5/17/10 same day (auto)</td>
<td>pending</td>
<td>auto</td>
<td></td>
<td>a member of our customer relations team will personally review your correspondence and respond as soon as possible; due to current volumes, response time is longer than normal given your situation, you can call our cust. Relation team: 877.228.1327</td>
</tr>
<tr>
<td>United Airlines</td>
<td>05/17/10 web form</td>
<td>5/17/10 same day (auto)</td>
<td>pending</td>
<td>auto</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The Good, the Bad and the Ugly ...
The Good: Alaska Airlines

- **Call #1:** 8 mins (on hold 3 mins)
  - very helpful, answered what she could, gave us number for corporate office to follow up on our unanswered questions
  - **Answer:** She explained that BoA provides their visa cards and is the only partner that receives PII;
  - **Question:** pertinent PII?
  - **Answer:** she was not sure, but told us what was associated with the Mileage Plan status (#, mailing info, #miles)

- **Call #2:** to corporate office
  - transferred to legal dept voicemail ... call to legal dept: directed to contracted employee who works with PP
  - **Answer:** Info used in reservations: name, travel itinerary; don't sell PII, and share info only in the case of customers registering for promotions/sweepstakes.

- **Total Length of Call:** 8 minutes w/ contracted employee on 6/8/2006
The Bad: Continental
3rd Party Data Retention

- "Continental contracts with reputable third parties to facilitate the collection and aggregation of Web usage and transaction information; the distribution of advertisements and electronic mail; and the operation of some survey, promotional and sweepstakes programs. Such third parties are subject to confidentiality and any necessary privacy requirements and, upon completion of these services, all information is returned to Continental."

- **Question:** How do you verify that these third parties actually destroy all copies of that information?

- **Answer:**
  - Wasn't sure at first (on hold for 3 minutes).
  - He had no info on this.
  - Did not have information on a customer service manager.
  - Said there was no place to go for an answer.
  - Was not aware of any compliance officer with whom we could speak.
Continental: Phone + Email Personal Data for Marketing

- "If you object to Continental maintaining and using your personal data for marketing purposes, OnePass members may opt out of such purpose by using continental.com (sign in is required)."

- **Question:** What specific personal information is used for marketing purposes?
- **Answer:**
  - would have to find out (put on hold for 7 minutes)
  - Belinda tells us that Larry Lettick (sp?) is not at his desk, but he is who we need to talk to
    - would not give us Larry's email or phone number, saying she wasn't sure if he wanted to be directly reached
    - offered to take our email and phone # to pass on to Larry - Annie gave her @purdue email address and @purdue phone #
  - call ended

- **Total Length of Call:** 10 minutes (7 minutes on hold) on 6/8/2006

- **Follow up response:**
- Email received (6/9/2006 @ 11:55pm from onepass@coair.com).
  Belinda Harris: "After speaking with the Corporate Security contact and our Marketing contact, I have been advised that we do not provide a specific list of all the data collected for marketing purposes. If you refer back to the PP on Continental.com, each section advises what information is collected. ..."
The Ugly: United Airlines

- 3 total calls, plus 3 total transfers
- **Call #1:** (customer relations): on phone 9 mins (on hold 6 mins)
  - refused to give name & number, said to call reservations to ask these questions
- **Call #2:** on phone 3 mins (on hold 2)
  - told to call web support w/ questions, had no info on compliance officer or legal dept #s
- **Call #3:** on phone 25 mins (on hold 10)
  - person said she wasn't the right person to talk to for any of the questions (in India);
  - asked to speak to supervisor (put us on hold for 2 mins)
    - came back & said "we don't share with gov't agencies or offices because you have a SSN"
  - can't give # for corporate office or legal dept
  - got very agitated at our questions and even yelled at us.
“Experts agree that good privacy begins with effective transparency. Transparency requires privacy notices that are easy to understand, facilitate comparison, and are actionable. Privacy notices must also comply with legal requirements ....” [www.hunton.com]
In Summary ...
Recommendations

- Construct meaningful, readable policies for your websites
- Consider alternative presentations of your policies
- Test your policies against focus groups
- Legalese is ambiguous and difficult to support
  - Compliance is easier to support with formalized methods
  - Analysis exposes ambiguities and choices to thwart potential abuses or privacy breaches
- Ensure people who may be contacted about your privacy policy are trained to respond in a meaningful way
Something we might consider here in the U.S. …
### 2006 Top Privacy Policy in Canada

In 2006, the awards for transparency go to:

<table>
<thead>
<tr>
<th>Banking</th>
<th>Telcos</th>
<th>Retail</th>
</tr>
</thead>
<tbody>
<tr>
<td>TD Bank Financial Group</td>
<td>TELUS</td>
<td>Chapters Indigo</td>
</tr>
<tr>
<td>Scotiabank</td>
<td>Telebec</td>
<td>Holt Renfrew</td>
</tr>
<tr>
<td>CIBC</td>
<td>Bell</td>
<td>Sears Canada</td>
</tr>
<tr>
<td>Laurentian Bank</td>
<td>Rogers</td>
<td>Costco Canada</td>
</tr>
<tr>
<td>RBC Royal Bank</td>
<td>Aliant</td>
<td>Roots Canada</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Financial Services (outside of banking)</th>
<th>Insurance</th>
<th>Media</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vancity</td>
<td>Aviva</td>
<td>CanWest Global</td>
</tr>
<tr>
<td>MCAP</td>
<td>First Canadian Title</td>
<td>Communications Corp</td>
</tr>
<tr>
<td>ATB Financial</td>
<td>LAWPRO</td>
<td>Thomson Nelson</td>
</tr>
<tr>
<td>Financialinx</td>
<td>belairdirect</td>
<td>Alliance Atlantis</td>
</tr>
<tr>
<td>GMAC Financial Services</td>
<td>Manulife Financial</td>
<td>Transcontinental</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Consumer Services</th>
<th>Business Services (outsourcing sector)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workopolis</td>
<td>Ceridian Canada</td>
</tr>
<tr>
<td>AIR MILES Reward Program</td>
<td>Ipsos Canada</td>
</tr>
<tr>
<td>Equifax</td>
<td>Aon Canada</td>
</tr>
<tr>
<td>TransUnion</td>
<td>ADP Canada</td>
</tr>
<tr>
<td>eBay Canada</td>
<td>Kelly Services</td>
</tr>
</tbody>
</table>


Ranking is based on transparency, not on content. For example, an organization that stated several uses of personal information for secondary purposes would rank equal to an organization that stated they didn't use personal information for secondary purposes. The key is providing notice on this matter.
Collaborators

- Faculty
  - Linda Aiman-Smith
  - David Baumer
  - Julie Earp

- Graduate Students
  - Davide Bolchini
  - Travis Breaux
  - Jack Frink
  - Qingfeng He
  - Neha Jain
  - Paul Otto
  - William Stufflebeam
  - Matt Vail

- Undergraduate Students
  - Carrie Gheen
This work supported in part by ...

- **National Science Foundation**
  - *Medium ITR Grant (2003-2007)*
    Antón, Earp, Baumer, Aiman-Smith, Stufflebeam, Jain @ NCSU
    Colin Potts @ Georgia Tech
  - *Digital Government Grant (2003-2005)*
    Antón, He @ NCSU
    José Fortes @ University of Florida
  - *Cyber Trust Grant (2004-2007)*
    Antón, Yu, Baumer, Rappa @ NCSU
    Elisa Bertino & Ninghui Li @ Purdue University
  - *ITR Grant (2004-2007)*
    Antón, Earp @ NCSU
    Elisa Bertino @ Purdue University

- **Computing Research Association DMP** (‘00,’01,’02,’04 ,’05)
- **NCSU Digital Enterprise**
- **IBM in RTP**
- **Purdue University CERIAS**
For More Information:

http://www.csc.ncsu.edu/faculty/anton

and

http://theprivacyplace.org/
Thank you!