

# Digital Transactions: Part Two: Assignment 11

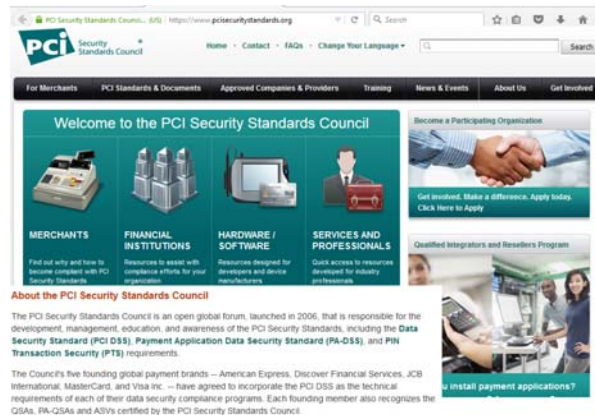
## Clickstream Data, Online Profiling, and Data Warehousing

- Data elements sent to a web site from the user's browser or computer
  - Applets enhance this capability
  - "cookies" / "web bugs"
- Tension: aversion to data collection (by some) versus economic value of the information
- Anonymizing tools



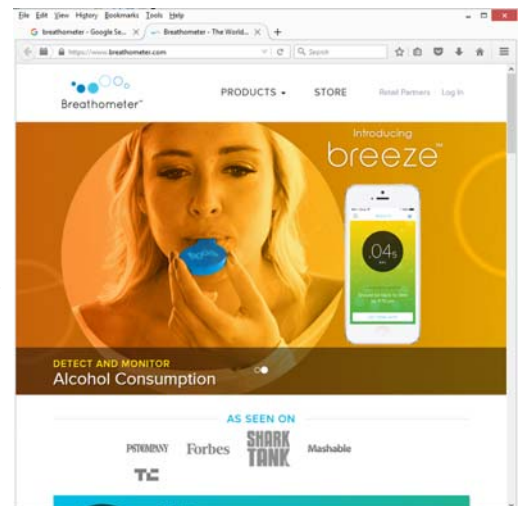
## Tortious Failure to Protect Data

- IT security practices by companies
- IT providers and flaws in the technology
  - And the continual release of updates driven by security issues
  - “best available security technology”
- Industry standards and/or best practices
  - Government references
  - Standards bodies
- Case Book emphasis on who is the “least-cost avoider”



## Peppet, Regulating the Internet of Things

- Internet of Things (IoT) (or, Internet of Everything)
  - A present reality
- Four technical challenges leading to four legal problems
  - Discrimination (“sensor fusion” and data-typing)
  - Privacy (difficult to de-identify)
  - Security (insufficient data security built into the designs of devices)
  - Consent
- Regulators need to respond with four preliminary steps:
  - substantive restrictions on use of data
  - consider biometric and sensor data PII
  - extend state data breach laws to IoT devices and promulgate data security standards
  - regulate a regime of IoT device privacy practices / disclosures

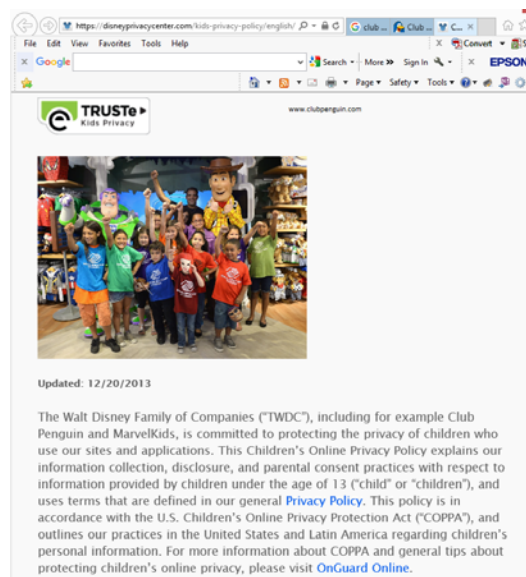


## Statutory Obligations to Protect Data: Fair Information Practices

- HEW
  - There should be no secret collections of personal data.
  - There should be a way for a person to find out what information has been collected and how it is used.
  - There should be a way for a person to prevent information that was obtained for one purpose from being used or made available for other purposes without the person's consent.
  - There should be a way for a person to correct or amend a record of identifiable information about the person.
  - Any organization creating, maintaining, using, or disseminating records of identifiable personal data should assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.
- OECD – 8 guidelines
- Boiling it down to: notice, consent, access, security (enforcement, chain of trust)

## Statutory Obligations to Protect Data: COPPA

- Web-site operators subject to the COPPA Rule must obtain "verifiable consent" from parents before collecting information from a child.
- The operator must send a notice to a parent informing the parent that it wishes to collect information from the child and that the parent's consent is required to do this, and then explain how the parent can consent. The notice requesting consent to the collection of information must include the same information as the posted privacy policy.
- To meet the standard of "verifiable" parental consent, the Web-site operator must make reasonable efforts in light of currently available technology to ensure that the child's parent has actually been notified and has consented



Updated: 12/20/2013

The Walt Disney Family of Companies ("TWDC"), including for example Club Penguin and MarvelKids, is committed to protecting the privacy of children who use our sites and applications. This Children's Online Privacy Policy explains our information collection, disclosure, and parental consent practices with respect to information provided by children under the age of 13 ("child" or "children"), and uses terms that are defined in our general [Privacy Policy](#). This policy is in accordance with the U.S. Children's Online Privacy Protection Act ("COPPA"), and outlines our practices in the United States and Latin America regarding children's personal information. For more information about COPPA and general tips about protecting children's online privacy, please visit [OnGuard Online](#).

## Assignment Eleven Problems

- 11.1 to 11.3