Access Control is an Inadequate Framework for Privacy Protection

Lalana Kagal & Hal Abelson
DIG @ CSAIL

Alternate Definitions of Privacy

- In 1890, Brandeis and Warren defined privacy as the "right to be let alone"
- In 1986, Alan Westin's seminal work described privacy as the ability for people to determine for themselves "when, how, and to what extent, information about them is communicated to others".
- The UN Declaration of Human Rights stipulates that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation".

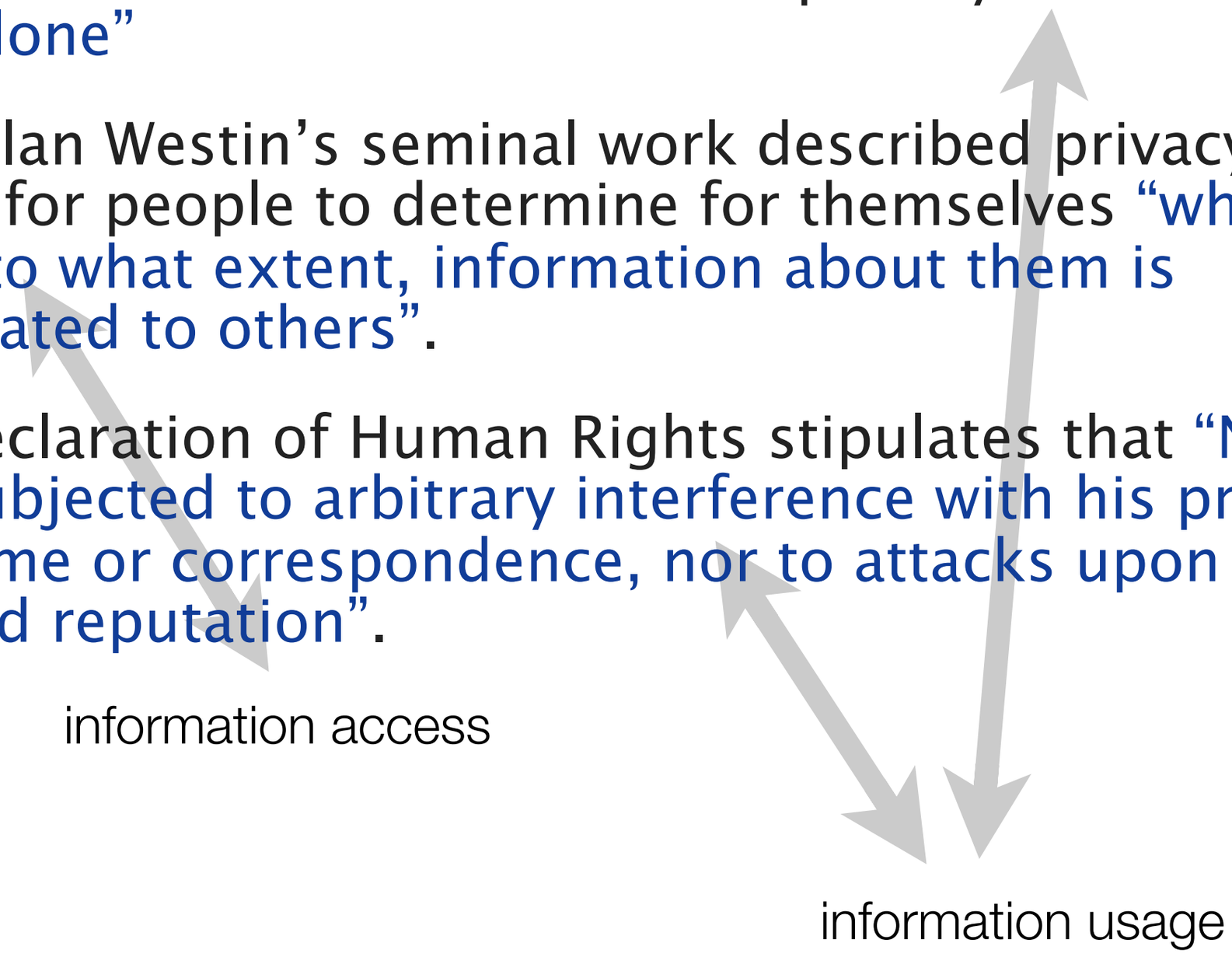
Alternate Definitions of Privacy

- In 1890, Brandeis and Warren defined privacy as the "right to be let alone"
- In 1986, Alan Westin's seminal work described privacy as the ability for people to determine for themselves "when, how, and to what extent, information about them is communicated to others".
- The UN Declaration of Human Rights stipulates that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation".

information access

Alternate Definitions of Privacy

- In 1890, Brandeis and Warren defined privacy as the "right to be let alone"
- In 1986, Alan Westin's seminal work described privacy as the ability for people to determine for themselves "when, how, and to what extent, information about them is communicated to others".
- The UN Declaration of Human Rights stipulates that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation".



Privacy = Access Control ?

- What's wrong with Westin's perspective of privacy
  - People exchange sensitive information in return for better services online
  - Users are unable to grasp privacy implications
  - System is unable to prevent misuse of data after authorized access
  - Sensitive information can be inferred from public resources

Image courtesy http://www.flickr.com/photos/sesh00/

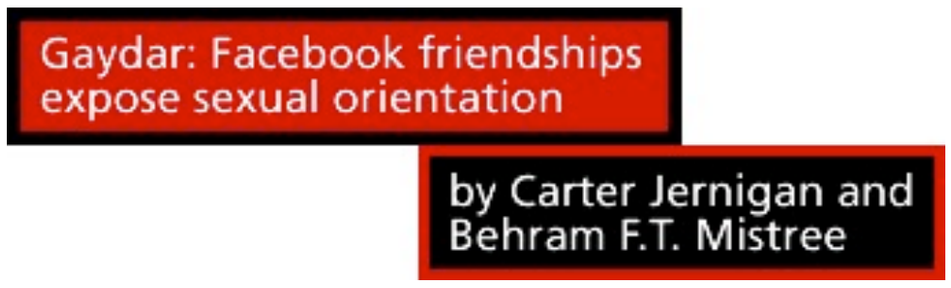


Image courtesy First Monday , http://www.uic.edu

Alternate Approach

- Brandeis and Warren perspective – focus on information usage
- Similar to how legal and social norms work in society
  - Signs and signals in human society describe expected/optimal behavior
  - Positive/negatives consequences of violating/ fulfilling the policy
  - Not always immediately enforceable – depends on type of policy and enforcement mechanism

Image courtesy http://commons.wikimedia.org/wiki/

Possible Techniques to Investigate

- Give users due notice
  - Google dashboard etc.
- Support information accountability
  - provenance
  - machine understandable policies
  - policy tools (reasoners, user interfa etc.)

Image courtesy Google Blog

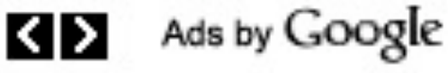


Image courtesy Google

Possible Techniques to Investigate

- Privacy-enabling Interface Design
  - Policy-awareness
  - Privacy implications
    - privacy nudges, Google Mail Goggles, abvenance

Image courtesy Google Blog

Work on Data Usage and Accountability

- European Data Protection Supervisor
  - Establishes a process for ensuring that the data protection standards set out in Regulation 45/2001 are met and for people to ensure that their data protection rights have been respected
- OpenForum.com.au Privacy & Trust http://www.iispartners.com/PTP_working_paper.pdf
  - Suggest a framework with focus on accountability and auditing
- Centre for Information Policy Leadership (CIPL)
  - focus on transparency, conflicting national legal requirements, cross border data transfers, and government

Summary

- Future of privacy protection lies in ensuring responsible use of data !
- Items for discussion
  - Privacy = education + access control + usage control + regulation. Will this provide the privacy we require ?
  - Possible to have a completely technical solution to privacy ?
  - US vs EU privacy issues

References

- Access Control is Inadequate for Privacy Protection, http://www.w3.org/2010/api-privacy-ws/papers/privacy-ws-23.pdf
- This presentation, http://dig.csail.mit.edu/2010/Talks/0712-W3CPrivacy-lk/privacy.pdf
- Virgin Mobile Steals Teen's Flickr Photo For Ad Campaign, “Dump your pen friend”, http://www.switched.com/2007/09/21/virgin-mobile-steals-teens-flickr-photo-for-ad/
- Project Gaydar, http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2611/2302