Taylor Spencer
Social Issues in Computing
Ian Brooks
03/19/2013

Term Paper Outline

1. Introduction
    a) There have been many controversies involving privacy lately.
    b) Purpose of Paper
        - In this paper, I will look at data privacy on the Internet.
            - First, I will examine the legal side of the issue, discussing what information companies can and cannot collect from whom.
            - Second, I will try to present an idealistic view of how, in my opinion, things should be as it relates to privacy.
            - Last, I will reconcile that with the status quo of privacy on the Internet.
    c) Thesis
        - There is a huge gap between how privacy is on the Internet and how it should be, and there are changes that should be made to address this.
        - I suggest bringing about these changes through the pressures of competition.
        - Granted, there is the risk that after gaining market share, companies could collude to undo privacy progress, but I believe that introducing privacy through competition is the best approach for achieving Internet privacy without ruining the freedom of the Internet, which is one of the things that makes the Internet great.
2. Body
    a) Legal Requirements
        - In America
            - General Privacy Laws
                - The United States does not have any general privacy laws, but instead has specific privacy laws that apply to specific situations (Conger, Pratt, & Loch 2).

Taylor Spencer
Social Issues in Computing
Ian Brooks
03/19/2013

- Specialized Privacy Laws
  - HIPAA
    - Requirements
      - HIPAA requires entities covered under the law to obtain a person's written authorization before using or disclosing "Protected Health Information", as defined by HIPAA, except for activities related to "treatment", "payment", and "health care operations" (Nosowsky & Giordano 3–4).
      - "Protected Health Information" includes information, including demographic information, "relating to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual" (Nosowsky & Giordano 3).
    - Consequences for Violations
      - First offenses are punished with fines (Stanford 1)
      - Subsequent offenses are punished with 1 year in prison for simple violations, 5 years [in prison] for obtaining medical information under false premises, and 10 years [in prison] for selling medical data (Stanford 1).
  - ECPA
    - Requirements
      - Outlaws interception of wire, oral, and electronic communications, and prohibits the disclosure or use of such communications (Sipior & Ward 6).
    - Notable Exceptions
      - The "business use" exemption exempts employers whose monitoring can be shown to have a business purpose (Sipior & Ward 6).
      - The "prior consent" exemption exempts anyone who has notified the parties involved prior to the monitoring (Sipior & Ward 6).
      - These two exemptions keep the ECPA from providing a significant level of privacy to employee email communications (Sipior & Ward 6).

Taylor Spencer
Social Issues in Computing
Ian Brooks
03/19/2013

- COPPA
  - Requirements
    - Requires website operators collecting information from children 12 and under to:
      - Post a privacy policy (Delaney 6)
      - Provide notice directly to parents get parental consent (Delaney 6)
      - Allow parents to review personal information collected from children (Delaney 6)
      - Allow parents to revoke their consent, and delete information collected from their children at the parents' request (Delaney 6)
      - Not condition a child's participation in certain activities on collection of more personal information than is reasonably necessary (Delaney 6)
      - Establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of children's personal information (Delaney 6)
  - Effect on Market
    - Many websites, instead of complying with COPPA, forbid all children under the age of 13 from creating accounts (Madden et al. 6).
      - Because of this, many children lie about their age to use these sites, sometimes with the help of their parents (Madden et al. 6).
- TCPA
  - Requirements
    - The Telephone Consumer Protection Act, or TCPA, regulates the use of automatic telephone systems and prerecorded calls and requires telemarketers to maintain "do-not-call" lists (Sorkin 1).
    - The TCPA also bans the sending of unsolicited advertisements to fax machines (Sorkin 1).

Taylor Spencer
Social Issues in Computing
Ian Brooks
03/19/2013

- CAN-SPAM Act
  - Requirements
    - The CAN-SPAM Act requires that email marketers label their messages as advertisements, include an Internet-based opt-out feature for the recipient that is active for 30 days, and provide the marketing company's physical mailing address in the message (Lee 1).
  - Consequences for Violations
    - Spammers caught in violation of the Act face "significant financial penalties" and "possible jail time" (Lee 1).
  - Effect on Market
    - The CAN-SPAM Act has had very little effect on spammers, since most spammers are unscrupulous people who use spam to send out viruses (Helman 4).

- Foreign Requirements
  - EU Data Protection Directive
    - Requires that consumers give clear consent before information may be collected or shared (Hiller 12)
    - Requires that data collection be "fair and legal", "for a specific purpose", "limited to the stated purpose", "accurate", and "stored only for the necessary time period" (Hiller 12)
    - Limits the sharing of information with entities outside the EU with countries that don't have an "adequate level of protection" (Hiller 12)
      - Because of this last requirement, the United States Department of Commerce had to establish a "Safe Harbor" agreement with the EU (Hiller 12).
        - This agreement states that in order to collect information from customers in the EU, companies must meet the "seven information practice principles of notice, choice, onward transfer, access, security, integrity, and enforcement" (Hiller 13).
        - Additionally, companies must also either be part of a "self-regulatory organization", or develop their own "self-regulatory compliance program" (Hiller 13).

Taylor Spencer
Social Issues in Computing
Ian Brooks
03/19/2013

b) How Things Should Be

- Web sites should:
  - Be upfront about what they disclose and when.
    - As web sites privacy policies must be written in legalese to satisfy the lawyers, we cannot hope to do this there.
    - Instead, there should be some supplemental document that is presented to the user that accomplishes this purpose.
  - When this policy must change, the website should inform the user what is changing and why.
    - This notification should be done through a method that the user will notice, such as email.
  - Allow the user to use a reduced-functionality version of the website if they do not wish to agree to all the disclosures.
- Web sites should not:
  - Revert their users' privacy settings every time a new feature comes out.
    - If a user's choice of privacy settings prevents a user from being able to use a new feature, the user should see a message every time they attempt to use that feature.
    - I know this sounds like common sense, but there is one company that does almost every time they introduce a new feature.
  - Allow one user to disclose another user's information.
    - Different users place different values on their privacy, and sites should respect that.

c) The Status Quo

- Facebook
  - Applications
    - Facebook allows applications to access profile information not just for that user, but for all of that user's friends, and send that information to a third-party server (Hull, Lipford, & Latulipe 7).
    - Since Facebook applications share information not just about that user but about that user's friends, a user's privacy can be violated by one of their friends without them being involved (Hull, Lipford, & Latulipe 8).

Taylor Spencer
Social Issues in Computing
Ian Brooks
03/19/2013

- New Features
  - As Facebook adds new features, the privacy settings for these new features default back to the "all networks" settings (Strater & Lipford 6).
  - News Feed
    - Through the introduction of the News Feed, Facebook put information that was already accessible in front of users, "reducing the de facto privacy of its users" (Hull, Lipford, & Latulipe 9).
  - Beacon
    - Introduced in late 2007, Facebook Beacon recorded the actions of Facebook users on 44 partner websites and posted them to the user's Facebook wall for their friends to see (Briggs 6).
    - After users complained that Facebook was publicizing their actions, including Christmas shopping (Dwyer 3), to their friends without their approval, Facebook changed Beacon to allow users to opt out of sharing (Briggs 6).
    - By then, Beacon had triggered a class-action lawsuit, and Facebook was forced to shut Beacon down and establish a $9.5 million settlement fund for "projects and initiatives that promote the cause of online privacy, safety, and security" (Dwyer 3).
- Google
  - Street View Wi-Fi database
    - In May of 2010, Google had to remove its Irish Street View fleet because its cars were collecting data submitted over Wi-Fi networks found in Ireland (Power et al. 10).
  - Google Buzz
    - In February of 2010, Google introduced a new feature in Gmail; a social network (Helft).
    - Users were angered that Google Buzz made something that was once considered private, email, and made it public, that their contacts list was being turned into a list of friends, and by the lack of privacy controls on the new service (Helft).
    - This caused several users to file a class-action lawsuit over Google Buzz, and Google was forced to pay $8.5 million in compensation to users for breaching user privacy (Dillon Scott).

Taylor Spencer
Social Issues in Computing
Ian Brooks
03/19/2013

- DNT
  - Google was found to have been bypassing the privacy settings of Safari (Angwin & Valentino-DeVries) and Internet Explorer (Steven Musil) users to track their browsing across the Internet.
  - As this case is a little over a year old, it is unsure whether Google will face any consequences for this.
- Other Companies
  - On September 19, 2003, JetBlue admitted that it had provided the travel records of five million customers to Torch Concepts, a DoD contractor, as part of an antiterrorism study to track high-risk passengers or suspected terrorists, in violation of its stated privacy policy (Anton, He, & Baumer 1).

3. Conclusion

a) There is a great gap between how privacy is on the Internet and how it should be.

b) However, before anyone suggests a comprehensive law, I suggest that they look the effects of COPPA.
   - COPPA was essentially the same kind of law but applied to children.
   - Because of COPPA, preteen kids cannot legally use many of the services we use and love, leaving kids stuck in a Web 1.0 world while everyone else advances on to Web 3.0.

c) A better way to bring about these changes is through the pressures of competition.
   - An example of this playing out today can be seen with a new search engine called DuckDuckGo.
     - This search engine has positioned itself in the market as a privacy-friendly alternative to Google, and as of early 2012, their growth has been surging, with average queries up 227% (Robin Wauters).
   - If companies learn that being proactive about privacy can allow them to gain market share, eventually all companies will adopt better privacy policies, not because of legal threats, but simply to stop losing market share to privacy-conscious competitors.

d) Secondly, legislation comes with the risk of over-regulation, or placing requirements on Internet companies that are impossible to fulfill in certain fields, shutting down services in those fields.
   - Introducing privacy through competition has none of these risks, since the fact that one company could adopt the privacy differentiator proves that it can be done.

Taylor Spencer
Social Issues in Computing
Ian Brooks
03/19/2013

e) Granted, there is the risk that after gaining market share, companies could collude to undo privacy progress, especially if market share figures have changed to the point where companies no longer see a competitive advantage in respecting privacy.

- But, for the reasons stated, I still believe that introducing privacy through competition is the best approach for achieving Internet privacy without ruining the freedom of the Internet, which is one of the things that makes the Internet great.