Privacy-Protecting Policies

Simson L. Garfinkel
The Big Idea:

Many technical problems can be solved through the use of policy.

Technologists tend to overlook policy solutions because they:

- Aren't 100% effective
- Don't work across legislative boundaries
- Are open to [possibly intentional] misinterpretation

Example: CAN-SPAM act
On the other hand...

Policy solutions can be more flexible than technical solutions

- Policy can be “technology-neutral”
- Policy doesn’t need to be upgraded
- Policy doesn’t crash when there are typos
- Policy can enable lawsuits that attack the human root of problems
The “Bad People” problem

- The world is filled with bad people.
- You can’t put them all in jail.
Evidence of “bad people”

- Decreasing inventory at stores
  - Shoplifting?
  - Employee theft?
- Merchandise purchased with “lost” credit cards
  - Perhaps the card was stolen
  - Perhaps the card wasn’t stolen
More Evidence...

- Money borrowed and not repaid
- Faked insurance claims
- Forged checks
Solution to the “bad person” problem

- Make a list of the bad people.
- Don’t do business with anybody on the list.
Examples of Solution...

- Retail Credit
  - List of people “known” not to reply their debts
- Medical Information Bureau (est. 1902)
  - List of people with “known” medical problems
- Chicago-area merchants (1950s)
  - List of “known” shoplifters
“Retired Army Lieutenant Colonel”
- “A rather wild-tempered, unreasonably, and uncouth person… who abused his rank and wasn’t considered a well-adjusted person.
- “He was known to roam the reservation at Ft. Hood and shoot cattle belonging to ranchers who had leased the grazing land from the Army.”

—Hearings on the Retail Credit Company, 1968
Credit reports of the 1960s

- Contained information that was hearsay or just plain wrong.
- Records confused between individuals.
- No “statute of limitations” on the information.
- People frequently prohibited from seeing their own records.
Fair Credit Reporting Act, 1970

- Right to see your credit report.
- Right to challenge incorrect information.
- Information automatically removed from report after 7 years
  - 10 years for Bankruptcy.
- Right to know who accesses your report.
- Right to a free credit report if you are denied credit.
Code of Fair Information Practices (1973)

- There must be no personal data record-keeping systems whose very existence is secret.
- There must be a way for a person to find out what information about the person is in a record and how it is used.
- There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
There must 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 must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.
CFIPs in Short

- No Secret databanks
- You are allowed to see your own record
- Information obtained for one purpose can’t be used for another without consent.
- Ways for correcting or amending information.
- Prevention of misuse.
CFIPs...

- Good ideas --- matches what we believe.
- FCRA - 1970
- 1980 OECD Guidelines
- 1999 Canada “C6”
- FTC’s “Notice, Choice, Security and Access”
Approaches to Privacy Enforcement

**Governmental Standards**
- Enforcement by regulatory agencies, states, etc.

**Industry Standards**
- “Codes of conduct”
- Limited enforcement through licensing
- Limited enforcement from government

**Unregulated Market**
- Reputation, or Caveat emptor
“Privacy” in the US, Last Few Years

Some Legislation
- HIPAA — Health Insurance Portability and Accountability Act (1996)
- COPPA — Children’s Online Privacy Protection Act (1998)
- GLB — Gramm-Leach-Bliley (Final rule, May 24, 2000)

Many Missed Opportunities
- S.2201 - “Online Personal Privacy Act”
RFID Bill of Rights

Why? Because RFID poses unique threats.
- Radio waves are invisible
- Tags and readers can be hidden
- Creepy Factor

Why? Because regulation is uniquely positioned to deal with a threat that includes:
- Legitimate companies
- Multiple frequencies and standards/non-standards
What’s the problem?

- MIT put a chip in my ID card
Questions about my chip...

- Does it have my name on it?
- Who has access to the database?
- How far can my card be read?
- What’s the “security”?
- What about cash purchases?
- Where are the readers?
- What’s done with all of the data?
And RFID “bill of rights.”

- Users of RFID systems and purchasers of products containing RFID tags have:

  1. The right to know if a product contains an RFID tag.
  2. The right to have embedded RFID tags removed, deactivated, or destroyed when a product is purchased.
  3. The right to first class RFID alternatives: consumes should not lose other rights (e.g. the right to return a product or to travel on a particular road) if they decide to opt-out of RFID or exercise an RFID tag’s “kill” feature.
  4. The right to know what information is stored inside their RFID tags. If this information is incorrect, there must be a means to correct or amend it.
  5. The right to know when, where and why an RFID tag is being read.
Example 2: Gator and GAIN

- **GATOR eWallet?**

- “The Gator eWallet is provided free by GAIN Publishing.”

- “The Gator eWallet is part of the GAIN Network.”

- “This software also occasionally displays pop up ads on your computer screen based on your online behavior.”

---

By GAIN Publishing

GATOR® eWALLET
THE SMART ONLINE COMpanion

- Fills in FORMS with no typing!
- Remembers PASSWORDS automatically
- Protects and encrypts your data on YOUR computer. Only your first name, postalzip code, and country are sent to GAIN Publishing. Click here to read our Privacy Statement.

Click here and get the Gator eWallet with no GAIN Network advertising for $30.
The Gator eWallet is provided free by GAIN Publishing. The Gator eWallet is part of the GAIN Network. This software also occasionally displays pop up ads on your computer screen based on your online behavior.

The GAIN name and/or logo are displayed on all GAIN Network ads, so you'll know they're delivered by the GAIN Network, and are not brought to you or sponsored by the Web pages you may be viewing when the ads are displayed. For more information, please click here.

The GAIN Network is the world's largest in-context behavioral advertising network. The GAIN Network helps keep many popular software applications and websites free in exchange for delivering advertising, which is selected for display based on your online surfing behavior.

Click here for more information on the GAIN Network.

The GAIN Network is owned and operated by GAIN Publishing.
Gator...

Comes with Gator eWallet, Precision Time, Date Manager, OfferCompanion, Weatherscope, and SearchScout Toolbar
Gator License Agreement...

Words: 6,645

Key Provisions:

- Displays pop-up advertisements.
- Determines your interests by monitoring your web surfing behavior, including the URLs you type.
- Software updates itself.
- Any use of a “packet sniffer” is “strictly prohibited.”

PLEASE READ THE GAIN PUBLISHING PRIVACY STATEMENT AND END USER LICENSE AGREEMENT (COLLECTIVELY "Terms and Conditions") CAREFULLY AND MAKE SURE YOU UNDERSTAND THEM. THEY CONTAIN IMPORTANT INFORMATION THAT YOU SHOULD KNOW BEFORE ACCEPTING ANY GAIN-Supported Software (DEFINED BELOW). The GAIN Publishing Terms and Conditions describe the operation of the GAIN-Supported Software you are about to download and the terms and conditions that govern your use of this software. GAIN Publishing ("GP") provides you the opportunity to download a software product you desire at no charge or a reduced charge in return for your agreement to also download GP's software product which will periodically ...
People are *bad* at reading legal documents

Solution:
- Standardized Labels of product actions.
- Logos of special significance

---

### Nutrition Facts

<table>
<thead>
<tr>
<th>Serving Size</th>
<th>Calories</th>
<th>% Daily Value*</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 oz</td>
<td>100</td>
<td>9%</td>
</tr>
</tbody>
</table>

- **Total Fat**: 6g (9%)
- **Saturated Fat**: 5g (25%)
- **Cholesterol**: 0mg
- **Sodium**: 25mg (1%)
- **Potassium**: 0mg

**Total Carbohydrate**: 33g (11%)
- Dietary Fiber: 0g
- Sugars: 32g
- Other Carbohydrate: 0%

**Protein**: 1g

---

**Vitamin A**: 0%
- **Vitamin C**: 0%
- **Calcium**: 0%
- **Iron**: 0%

Percent daily value reflects "as packaged" food. Product is marked with a Kosher symbol.

* Percent daily values are based on a 2,000 calorie diet. Your daily values may be higher or lower depending on your calorie needs.

<table>
<thead>
<tr>
<th>Calories:</th>
<th>2,000</th>
<th>2,500</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Fat</td>
<td>Less than 65g</td>
<td>80g</td>
</tr>
<tr>
<td>Sat Fat</td>
<td>Less than 20g</td>
<td>25g</td>
</tr>
<tr>
<td>Cholesterol</td>
<td>Less than 300mg</td>
<td>300mg</td>
</tr>
<tr>
<td>Sodium</td>
<td>Less than 2,400mg</td>
<td>2,400mg</td>
</tr>
<tr>
<td>Total Carbohydrate</td>
<td>300g</td>
<td>375g</td>
</tr>
<tr>
<td>Dietary Fiber</td>
<td>25g</td>
<td>30g</td>
</tr>
</tbody>
</table>

**Calories per gram:**
- **Fat**: 9
- **Carbohydrate**: 4
- **Protein**: 4

---

**INGREDIENTS**: Sweeteners (High Fructose Corn Syrup, Sugar), Cream Of Coconut (Coconut Milk, Sugar, Water, Polysorbate 60, Sorbitan Monostearate, Salt, Xanthan Gum, Calcium Carrageenan, Sodium Alginate, Mono And Diglycerides, Citric Acid), Water, Crushed Pineapple, Concentrated Pineapple Juice, Less Than 2% Of Each: Natural Flavors, Xanthan Gum, Citric Acid (Provides Tartness), Potassium Citrate (Regulates Tartness).
1906 Pure Food and Drug Act

- Required disclosure of narcotics and other substances.
- “Warning --- May be Habit Forming”

(got the cocaine out of coca-cola)

http://www.cfsan.fda.gov/~lrd/history1.html
The Pure Software Act of 2006

- Hook: Starts automatically
- Dial: Places a Call
- Modify: Alters OS
- Monitors you when not active program
- Displays Pop-Ups
- Remote Control
- Self-Updates
- Stuck: Cannot be Uninstalled
Gator with Icons

(simulation)
Notes on the icons...

- Icons force disclosure of things that the lawyers might have forgotten. (e.g. 📜)
- Having an icon isn’t good or bad. (e.g. 🔄)
Summary

- Regulation can be your friend
- Regulation can do things that technology can’t
- Regulatory efforts need people who understand technology

Acknowledgements:

- Matthew Bouchard (icon design)
- Alma Whitten (mentioned warning labels in “Why Johnny…”)
- Rob Miller, David Clark, Min Wu, Steven Bauer (MIT)
- Jonathan Zittrain (Harvard Law)