Will People Ever Pay for Privacy?

Adam Shostack
adam@homeport.org

Presented at BlackHat Briefings
Amsterdam, May 2003
Overview

- The Importance of Privacy
  - What Is Privacy?
  - The Conflict
  - Lessons
- How to Include Privacy in Product Plans
- Conclusions
Does Privacy Matter?

- Polls say that it does
- Media reports pay it huge attention
- People seem to care quite deeply
They don’t act that way

- Tell strangers all sorts of things
- Don’t object to intrusive searches
- Don’t buy privacy products in great bulk
- Author worked for Zero-Knowledge for three years
  - Still in business, not ruling the world.
- “People won’t pay for privacy”
People Won’t Pay for Privacy

- Wrong Conclusion
- People won’t pay for things they don’t understand:
  - The problem a product solves
  - The way it solves it
- Freedom Network had both those issues
  - People were amazingly excited by the idea
Quick Review Freedom Net

- Zero Knowledge’s Anonymous IP net
  - Real time
  - Email, web, chat
  - No single trust point
  - Very expensive to operate (ZKS paid)
- No longer in operation
Privacy is Very Complex

- Includes Spam, ID theft, cookies, right to be left alone, informational self-determination, "lie and get away with it," and abortion
- Includes unobservability, untracability, data protection
- People pay for curtains, unlisted phone #s, and Swiss bank accounts
Privacy means too much

- The word has too many meanings
- People use it sloppily
- The result is confusion over what people want and will pay for
Overview

- The Importance of Privacy
  - What Is Privacy?
  - The Conflict
  - Lessons
  - How to Include Privacy in Product Plans
  - Conclusions
What is Privacy?

Confusing!
Privacy is Many Things

- Spam, telemarketers
- ID theft, CC theft
- Cookies
- Total Information Awareness
- CAPPS II
- Curtains & Venetian Blinds
- Do Not Call lists
- Fair Information Practices and Data Protection Laws
- Right to be left alone
- Informational self-determination
- “Lie and get away with it”
- Abortion
- Gut feelings
Broad Set of Privacy Tech

- Cash and banks
  - Athenian banks and taxation
- Remailers
- Fake ID
- Curtains
- Anti-spyware
Complexity vs Engineering

- Complex systems are hard to build
- Fundamental Security principle
- Privacy is a very complex issue
- Maybe the law can help?
Laws Much More Uniform

- Almost all built on Fair Information Practices
- Data Protection
- Tradeoff between
  - “You must give us this data”
  - “We’ll treat it fairly”
  - Mandatory tradeoff (one size fits all)
Overview

✓ The Importance of Privacy
✓ What Is Privacy?
  ▪ The Conflict
  ▪ Lessons
▪ How to Include Privacy in Product Plans
▪ Conclusions
Two Important Conflicts

- Data collection, protection, use
- Privacy is fuzzy and complex
Data Collection, Protection

- Business collects data for various good reasons
- Wants to maximize value from data
  - Legal in US
  - Data Protection law in “rest of the world”
- Individuals are often disempowered
Externalities

- A situation in which someone’s well-being is affected by another’s action, and they have no control of, or involvement in, that action
- Pollution is a classic example
Looking at the Externality

- Storage of data creates privacy hazard
- (Computer security stinks)
- Users are not in a position to insure against risk
  - Hard to measure value
  - Hard to measure risk
  - Risk is a likelihood of a hazard leading to damage
- May lead to tort claims
Risk & Externality

- Business are not motivated to protect data as well as the individual who will be hurt by its release
- AIDS patient lists
- Many people not comfortable with this tradeoff
  - “Privacy Extremists”
Both Sides Are Rational

- Business needs certain data to function
- Customer doesn’t trust the business
- Let’s not even talk about secondary uses (yet)
Both Sides Are Emotional

- People are tired of privacy invasions
  - Ask the travel business about CAPPS II
- Businesses are tired of privacy complaints
  - Ask your HR person for privacy problem stories…but only over beer.
Privacy is Fuzzy & Complex

- Many meanings of the word make it easy to talk about different things
  - Add to economic and emotional conflict
  - Good recipe for pain and suffering
Zero-Knowledge Experience

- Sold really cool Freedom Network anonymous IP service
- Consumers don’t understand online privacy invasion
- Consumers don’t understand “Anonymous IP”
Zero-Knowledge, cont

- It didn’t do well in the market
- What can we learn from this?

- NOT: “People won’t pay for privacy”

- Service didn’t meet a meaningful threat that the users cared about
Overview

✓ The Importance of Privacy
✓ What Is Privacy?
✓ The Conflict
  ▪ Lessons
  ■ How to Include Privacy in Product Plans
  ■ Conclusions
Match Threats and Defense

- Both real threats, and perceived ones
- Your collection and storage of data is a threat
- Don’t take that personally, its just economics of externalities
Threat: ID Theft

- Two major types:
  - Account takeover
  - Application Fraud

- Now an insurable risk

  - “time and money it takes you to wade though the logistical and legal paperwork.”
Account Takeover

- Consumers very aware of threat
- Collected carbons
- Visa: Don’t print entire CC # on receipt
- Matches threat & defense in customer visible way
- Doesn’t address storing CC# in db
  - May well be a worse problem
  - But not visible to consumer
Account Takeover (2)

- Digital Cash
  - Way cool technology
  - “Too much work for the consumer”
  - Actually, too much work because the consumer doesn’t see the benefits, just the cost

- Poor matching of defense to perceived threat
The Hell With It?

- If consumers don’t have a choice…
- Security vs privacy & the nature of trust
- Effort here will be rewarded
  - If it results in a visible difference
  - Laziness here exposes you to risk and customer hatred
  - Ask TRW Credit (formerly Experian)
- Talk to your regulators
Overview

✓ The Importance of Privacy
✓ What Is Privacy?
✓ The Conflict
✓ Lessons
 How to Include Privacy in Product Plans
■ Conclusions
Privacy Impact Assessment

- What are you collecting, and why?
- What are you storing, and why?
- What are you selling to your partners…
- PIAs now mandated in many places
- See
Beyond PIAs

- Minimize!
- The core consumer concern is that you’re not trustworthy
- Don’t argue, agree!
- “We don’t want your data!”
- Collect less, use it better
- Think from customer’s viewpoint
<Gavin> I hate those surveys they give
Gavin is a 102 year old Albanian reading the washingtonpost.com
<Smartboy> I’m guessing they think they have a great readership in Newton Falls, Ohio (Zip code 44444)
“What are you collecting, and why?”

WP is collecting demographics
- Probably to help sell ads
- Ad sales, prices keep falling
- Data that everyone knows to be bad can’t help

Comments at bottom were unprompted as I was writing presentation (IRC channel)
Your Personal Information

First Name: 

Last Name: 

Address: 

Apt. or Suite No.: 

SSN: [Redacted]

Date Of Birth: [Redacted]
State of Georgia

There is a problem with the certificate that identifies "idt.nw3c.org". Do you want to continue?

The certificate was issued by a certificate authority that Mozilla does not recognize.

- View Certificate
- Remember this certificate permanently

Continue  Cancel  Help
State of Georgia

- Deserves kudos for doing something
- Cold be more sensitive
  - Collecting everything needed to commit more ID theft in one place
- Very privacy sensitive audience
- No clear statement of what’s mandatory
- No clear statement of data use
  - (May be concealed in long legalese)
Overview

- The Importance of Privacy
- What Is Privacy?
- The Conflict
- Lessons
- How to Include Privacy in Product Plans
- Conclusions
Privacy is...

- Complex
- Multi-faceted
- A cause of heartache all around
- Manageable
Risk and Externality

- Promises won’t satisfy the growing privacy camp
- Understand the problem
  - Divide and conquer
- Turn it against your competitors
- Toolset for
  - Understanding
  - Improving