Internet Privacy – Policy Must Precede Technology
DON’T PUT THE CART BEFORE THE HORSE
SEVERAL OPEN QUESTIONS

What is tracking?

What is your threat model?

What are the Trade-offs

What can we learn from the past?
WHAT DOES TRACKING MEAN?

Fundamentally, this is a policy problem
- Informed by an analysis of technology, a constantly moving target

Multiple requirements
- Privacy rights and expectations of internet users
  - Balanced by property/security requirements of website operators.
- Jurisdiction issues
- Security/Fraud controls are needed to protect privacy online

User Expectations Vary
- Capturing intent/belief, especially implicit expectations, is hard
WHAT IS YOUR THREAT MODEL?

Are you worried about:

• Government Surveillance?
• Websites you have a direct relationship with?
• Online Advertisers?
• Data Brokers?

• Or....
• Online Hackers and/or Criminals?
A LITTLE STORY ABOUT TRACKING

Once upon a time a user had the username and password of their social network accounts compromised.

One of the social media companies let the attackers right in, no questions asked.

Another social media company noticed that many things were amiss and blocked the login.
- Time of day
- Source-IP
- Other client identifiers

As a user, which experience do you want?
WE ARE IN AN ARMS RACE

As Panopticlick showed, the browser is extremely leaky...
  • It was never designed not to be

Researchers find new ways to fingerprint browsers, implementation bugs, quirks, etc. all the time

Unlikely we will find a solution for the “average internet user”
  • Maybe we can solve this for those who need “true” anonymity
    • Dissidents, etc.
  • But probably at a very high cost
BE CAREFUL WHAT YOU WISH FOR

The tradeoffs between security and privacy don’t have to be a zero-sum game.

But sometimes we are forced to choose:
• Persistent HTTP Strict Transport Security (HSTS) across Private Browsing instances?
  OR
• Privacy-enhanced, but less secure, HSTS?

What is the right default? Who should decide?
THE PARADOX OF USER CHOICE

There is a conflict between user choice, and safe defaults
- History littered with attempted solutions

SSL Warnings
- And other web browser popups

Not limited to Computing
- Automatic Seatbelts
- Auto-locking dorm room doors?
PAST TECHNOLOGY-ONLY EFFORTS WERE ONLY PARTIALLY SUCCESSFUL

Cookies
- Technology implemented before privacy policy
- It got a lot of things wrong

P3P
- Makes arbitrary distinctions of security/privacy model based on domain names

“Private” browsing modes
- No clear definition
  - Protection from other local users?
  - Protection from sites that want to track across sessions?
  - Protection from Government?
MORE TRICKY PROBLEMS

NoScript
- Tries to implement safety rules
  - Default configuration at one time broke PayPal checkout flows because it prohibited cross-domain POST
- Tries to stop certain types of tracking/analytics
  - Has to go to great lengths to stop actual use of those JS functions

Secure Mashups
- If we want to allow these, we can’t have default rules that prohibit “third-party” cookies, authentication, etc.
PROGRESS IS BEING MADE

HTML5 Location
- A web standard for asking a user-agent for location data
- Fairly standard user-interface for asking for user consent

Still room for progress
- What are the user expectations?
  - Will my location be stored?
  - What else will it be used for?
  - How granular of location data does the server really need?
  - Should the client give a fuzzy answer?
PRIME DIRECTIVE: DON’T BREAK THE WEB

Solve the policy problem first
  – Build more universal security policies and easy to understand implementations

Don’t negatively impact Mashups, Security, or Anti-Fraud
  – Security of users
  – Security of sites

Solving today means incremental improvements, but beware of the trade-offs