Incentives and information flows in online identity

Seth Schoen
Electronic Frontier Foundation
June 28, 2011
... do these parties *actually agree* about how information should flow?
Congruence of individual's and relying party's desires

• Wells Fargo Bank sent me an RSA SecurID token, at my request, to secure access to my bank account

• Wells Fargo and I both agree that this is preferable to password-only authentication for EFTs from my account
NSTIC aspires to a world of harmony on this point

• “Relying parties shouldn't ask for more information than they need”

• …
Gaps between user's and other parties' desires

• Yesterday Google sent me this PREF cookie:

ID=bd2227be51143a4e:TM=1309185417:LM=1309185417:S=1jbD5rpx67lQu3YZ
The gap

- New online identity mechanisms are great for users' interests when users and RPs have similar goals about the “desired” or “appropriate” level and kind of authentication or identification
  - Especially attribute-based systems like Microsoft's U-Prove

- But this is only sometimes true!
Authentication vs. identification

• One example is that we might prefer to be very strongly authenticated without being identified at all (with PII)

• We may want to protect accounts against unauthorized access and use, without revealing who own them

• People may call this “anonymity”, but it's strictly pseudonymity
Effects of ID mechanisms

• ID providers learn & store transactional, location data (Aaron Titus)

• Trust framework rules are not necessarily aligned with end-user preferences
  – E.g., credit card transactional data is governed by rules but they don't let me get it destroyed quickly
Effects of ID mechanisms

• Increased pressure to provide identity in new contexts, more difficulty resisting or evading identity demands

• Attribute proving could enable proof demands in new contexts by making them seem more reasonable or less intrusive
Incentives question

• You may have a very different notion of what information some entity “needs”

• Aaron Titus: the FIPPs *don't judge uses*

What incentives will IDPs and RPs really have to align their information collection and ID demands with end users' preferences?