Berkeley Law
University of California
Samuelson Law, Technology & Public Policy Clinic

Keyna Chow, Nick Petersen, Chris Hoofnagle
Objectives

• From the prospective of a lawyer
• Technology informed Policy
  – & Policy informed technology
• Highlight shortcomings in self-regulation programs that are relevant to Do Not Track
• Work thus far:
  – Comments to EASA
Don’t let weasel words eat away privacy protection!

Behavioral Targeting

*must be:*

“Web viewing behaviors”

“from a particular computer”

“across non-Affiliate Web sites”

Ad Delivery & Reporting + other uses not covered

“Ad Delivery is the delivery of online advertisements...” basically almost everything else not “covered by the definition of Online Behavioral Advertising.”

PII is “information about a specific individual...”

Sensitive Consumer Information is “Precise Information...about health or medical conditions...”

What about non-OBA tracking?
Questions for Technologists

• Can you think of a creative solution that allow Ad Delivery and Reporting without tracking consumers?

• If Ad Delivery and Reporting falls outside the scope of Do Not Track, how can we use technology to verify that the data collected is used for Ad Delivery and Reporting only, but not for any other purposes?
Limitations on Consent

• Consent is not binary
• What, if any, protections should be in place for those who consent?

Football: Players consent to certain types of physical violence – but not all physical violence.

Do Not Track: What scope of business activity is given a green light?
Scope of Consent for Data Retention

• Data retention “only as long as necessary to fulfill a legitimate business need . . . ”
  – DAA and NAI self-regulatory principles

• Probably diminishing returns and costs associated with retention

• Network operators: Usually say they need data for short periods of time (as opposed to OBA lobbyists)
Anti-Circumvention of User Choice

• "[T]he practice of using technologies in order to circumvent the user’s express choices (for example by deliberately “re-spawning” deleted cookies), is not regarded as compliant with data protection law and should not be used.”
  – European Advertising Standards Alliance

• Why not in the NAI and DAA principles?
• Can DNT detect user circumvention?
Conclusions

• Technology & policy necessary
• Self-regulatory gaps will be relevant for implementation of Do Not Track
  – How do we use technology to enforce that data collected for analytics is not used for other purposes?
  – Can DNT protect consumers after they’ve consented?
  – Can DNT detect/enforce retention policies?
  – Can DNT address circumvention problems?