Technical Tools for Legal Consent: Do Not Track Meets the Needs of GDPR & CCPA Consent Rights

Frederik J. Zuiderveen Borgesius, Radboud University, Nijmegen & University of Amsterdam; Aleecia M. McDonald, Carnegie Mellon University

What’s wrong with this picture?

• No way to decline consent – lonely “I agree” is not a choice!
• Not clear and unambiguous.
• Acknowledges third parties, but never names them.
• Cookies set immediately, before consent is requested.
• Likely illegal under European GDPR law (pending case)
• No opt-out button as required by California’s CCPA law.
• If users agree, consent is saved indefinitely. If users do not agree, they are pestered repeatedly.
• Not only is this specific user interface deliberately unusable, a web full of these dialog boxes on multiple websites is pointless, frustrating, and makes a farce of the notion of privacy choices and privacy laws.

A better path forward

• Use a Do Not Track browser-based HTTP signal for consent.
• Users set a default choice once. Rather than improve consent experiences, can largely eliminate pointless cookie notices.
• Companies can ask for specific exceptions. Need to limit this to a reasonable frequency of requests.
• Live implementations are already close to Europe’s GDPR and California’s CCPA requirements, even though some implementations pre-date recent laws.
• Europeans and Californian children under 13 must opt-in to tracking. Adult Californians must opt-out of tracking. California teens between 13 and 16 must opt-in, with consent from teen or parent. Do Not Track cannot tell a user’s age, but can work with multiple opt-in or opt-out frameworks.
• Proven to work at web scale.

What’s at stake?

• **Financial impact**: estimated $333 billion spent on ads in 2019. Google captures nearly one third of revenue. Challenge: preserve economic value while enabling privacy choices.
• **Democratic elections**: targeted ad data used in Brexit and US 2016 Presidential campaigns by Russians to suppress turnout, undermine faith in the process, and create social divisions.
• **Surveillance**: the National Security Agency (NSA) used Google PREFID tracking cookies to hack track, then hack targets. NSA bought Google ads to strip anonymity from Tor users.
• **Trust**: Pew finds over 90% of Americans believe consumers have lost control over how personal information is collected and used by companies.
• **Privacy rights**: intrinsic harm independent of applications.

Challenges

• History shows companies do not have incentive to design usable consent mechanisms.
• Apple removed Do Not Track from Safari over fingerprinting concerns, despite low entropy.
• Likely requires additional laws, case law, or regulations.
• Future work: understanding users’ current mental models of consent, designing new consent mechanisms, and testing the usability of consent dialogs to get it right.
• Precedent and guiding examples: Schumer box for disclosing credit card rates, as required by law, and designed with extensive study of usability.