Usable Consents

Tracking and Managing Use of Personal Data With a Consent Transaction Receipt

Mark Lizar
Open Notice Initiative
London, UK
Mark.lizar@gmail.com

Abstract
Privacy and terms of use policy infrastructures on the Internet are broken.

Fixing the broken aspects of digital life is critical component to safeguarding freedom and protecting privacy for society.

We propose creating an Open Notice and Consent Receipt architecture, as a part of public data control infrastructure, (including both the social web[i] and other digital life access points) in order to open the closed and custom format of policies and consents currently used. We believe this can be achieved with a common digital Consent Receipt Format standard. We hypothesize that this format, structured with the links to legally required consent notices across jurisdictions, will open up control of personal data in simple but usable way.

Author Keywords
Notice & Consent; Privacy; Personal Data; Consent Receipts; Open Notice; Usable Consent; Terms of Use;

Open Notice Initiative Background
The Open Notice group started in 2012, growing into an Initiative designed to address the practical issues in notice and consent so as to enable meaningful choice. A paper was presented by Open Notice to the W3C Conference ‘Do Not Track and Beyond’ in 2012.[ii]

In 2013, the Open Notice Initiative started working on a market based approach addressing the lack of openness to consent and the data it controls.

Our response has been to promote, evangelize and develop Usable Consent, starting with the development of a standard 'Consent Receipt' schema. The Consent Receipt as a concept is best understood as a co-regulatory framework. Similar to regular money-based transaction receipts, but consent centric, they are designed to be digital and easily aggregated. Most importantly, a Consent Receipt is provided to the individual so that people can autonomously manage consent preferences and make choices on aggregate, similar to the way organizations give us transaction receipts. Consent Receipts can also be generated independently of the service provider infrastructure through personal apps, using an open-standard schema by way of links provided in a receipt.

Introduction

Before the rise of consumer rights and market regulations, the general rule for individuals making commercial transactions was caveat emptor ('buyer beware'). But even before consumer protection law, protecting consumers where their purchases were unrecorded and untraceable was impossible. The very first writing example we have, and what writing was invented for, is a transaction receipt.[iii] Humans have wanted to document our agreements since the very beginning. Over time, formal rules and systems evolved to provide consumers with open and fair standards and practices for proof-of-purchase receipts. This open and consistent transaction receipt has grown to co-regulate the commercial market and has formed the bedrock for trust, autonomy and freedom from abuse; as people, organizations and regulators can use them to self enface terms of the transaction and independently manage common disputes. The current personal data economy has returned us to the stone ages as far as our agreed upon methods for documenting transactions. Consent Receipts attempt to protect individuals' personal data from abuse and empower them with their own data to create an equivalent bedrock between parties. For this, usable consent can be achieved with a receipt infrastructure, providing data control transparency and meaningful choice.

The Consent Receipt project seeks to enable and ensure personal data control transparency by building up the infrastructure of personal data control for people (which is lacking compared to the sophisticated and already developed digital infrastructures and policies exploited by organizations today in a one-sided manner). The Open Notice Initiative does this under the premise that personal data control is a key component to contemporary agency and information autonomy. As Evengy Mogorov talks about in 'The Real Privacy Problem', privacy is a means to an end, not end in and of itself.[iv]

Agency over personal data is instrumental to personal autonomy and choice in participation of democracy and the exercise of freedoms. These chilling effects due to the surveillance state are well documented.[v] [vi] In order to enjoy privacy, personal data control promises to balance the trend toward 'algorithmic regulation' that big data creates with private analytics realized through personal data control in the future.

The Problem

The Open Notice community has identified legal and rights-based flaws as explained in the paper "Open Notice: A Call For Collaboration" presented to the W3C, Do Not Track And Beyond conference.[vii]

In short, our personal data is shared under the legal pretext that it will be protected by terms of service and privacy policies that are to some degree regulated by privacy and data protection law. This is not the case.

Research has shown that the existence of a privacy policy often leads people to believe their data is more protected, when the opposite is generally true. "In a way, consumers interpret (a) privacy policy as a quality seal that denotes adherence to some set of standards."[viii] When companies use this information beyond the stated purpose originally agreed to, and outlined in their terms of service and privacy policies, or what the law allows (such as selling it to a third party), services often act in violation of established personal, cultural and social convention. Often policies materially change over time and the data subject has not been asked for additional consent to these changes. Without compliant notice and choice, the use of data violates privacy regulation, contravenes multiple privacy principles, and disregards the spirit of legislation found in regional, national and international law. It is now clear that an honor system for data control that is self-regulating is ineffective.

Furthermore, the closed notice and data control practices are threatening to create 'invisible barbed wire' around our intellectual and social lives. Big data, with its many interconnected databases that feed on information and algorithms of dubious provenance, threaten to impose severe constraints on how we mature politically and socially.

Usable Consent

People suffer from all sorts of issues resulting in their need to make on-the-spot decisions for consenting to share information in ways they cannot predict or imagine. Many factors come into play for individuals trying to assess whether to consent: context, time of day, amount of sleep, number of activities at once, compelling temporary need to solve a problem, as well as lack of transparency or understanding systems that

use data. People are notorious for making poor decisions when pressed by other concerns, and very much require the facilities to manage consent outside of the context it was provided.

Privacy principles, existing law and the Individual require a framework permitting people to collect all of the privacy/security/trust assertions within a structure that is easily organized in a personal email or cloud or other storage system. This requires the ability to store those assertions (captured in receipts) in a manner that is searchable by the individual and understandable by the party who made those promises.

The Usable Consent framework creates transparency through open, interoperable, inclusive and viable standards to facilitate substantial participation by all stakeholders. For example, it must be an individual's choice about whether to store privacy promises on a personally owned device or in the cloud and to move them whenever they wish. And data handlers require the ability to update policy changes and therefore need a system to request further consent to use permissioned data for more granular data actions and administrate preference change requests.

Usable consent will simplify policy in a meaningful way for people by showing them simple privacy icon methods to display visualizations of complex policies, to be quickly scanned and decided upon. Consent Receipts will facilitate and further open a market for reports and data control intelligence for all stakeholders. A Consent Receipt is easily built into existing and already global consent and choice infrastructures found online. For example, Consent Receipt systems can sit behind an existing consent button or opt-in, in the browser, as a mobile device application, built into the operating system of a device, or even programed directly into the hardware of IOT devices and the like.

Consent Receipts function to record all of the privacy and terms of use policies put forth by companies and institutions, individuals' consent preferences, to link to required legal notices for different jurisdictions or types of data, and to link to the functional controls for managing the control of data and consent. For example, a Consent Receipt would record a Do Not Track signal in such a manner to memorialize the transaction. Copies of this Receipt are then provided to all parties, and individuals can choose to send their copy to a personal data store or email or other repository. In some cases, it is possible that both the data collector and the data subject will act to create and share these Consent Receipts, depending on the scenario. And with a Consent Receipt, the Data Controller (ie. the service provider or data collector) and the Data Subject (ie. the individual providing data) are able to more easily switch roles, enabling the Data Subject to effectively act as their own Master Data

Controller for themselves, by controlling their own personal cloud and collecting their own data.

Although Consent Receipts are different than transaction or purchase receipts, an individual could choose to maintain a local registry of their own consents, as well as to publicly share aspects of the Consent Receipt with the Open Notice consent registry and other social media. This kind of sharing will allow the public, regulators, press and individuals to see how consent works for others, without seeing personal information, because of the aggregated nature of the sharing.

Open Notice Initiative plans to develop a distributed receipt registry for public and private use, through open specifications, open source software and by inviting collaboration with other projects in this field such as privacy icon projects. With this approach, basic reporting tools will help all stakeholders, providing the structure to aggregate consent centric activities and visually understand them according to context.

We believe when the structures to control personal data are opened, privacy and trust icons can be easily mapped to context, so that protocols like P3P can utilize receipts to communicate preferences and inherently make transparency more actionable.

Scope and Interoperability

The Open Notice Initiative oversees development of common protocols for Consent Receipts, develops open source tools with this standard, and endeavors to facilitate, support and interoperate with many existing and emerging projects in this field. However, we will not build the usable privacy or policy visualizations needed to convey an organization's data governing policies (ie. privacy, cookie, terms of use (TOU) or other wise). We will partner with Privacy Icon projects to facilitate this functionality.

A Consent Receipt, like a transaction receipt, is in essence a vehicle for noticed information, although as a digital notice it also links consent controls and channels policy information to the individual. And because the Consent Receipt records the control of consent (like a monetary transaction) it creates a market for accountability and facilities the auditing of services.

The Consent Receipt, digitally usable as a consent token for other services and service memory, provides the missing infrastructure for usability in the identity management ecosystem, freeing the management of each individual profile from the control of silo’d platforms.

Conclusion

Opening up data control with Usable Consent and Consent Receipts is an approach that aims to evolve the legacy consent and notice infrastructure online in a fundamental and striking way. It is a proposal to create building blocks for addressing compliance, data control and usability issues with higher quality of consent management.

The Consent Receipt proposes an independent data control system: a system for exposing privacy icons at the point of consent, recording short notices to create usable privacy. All parties in a transaction will be properly noticed through the Consent Receipt, facilitating the Co-regulation of data control. We believe a fundamental sea change will occur where regulators and the public will have insight into previously opaque notice and consent systems, allowing for market pressure, public and social pressure, and the enforcement of current regulations to help the individual and society rebalance privacy interests.

REFERENCES

[1] *W3C, W3C Incubator Group Report 6th December 2010, 'A Standards-based, Open and Privacy-aware Social Web' http://www.w3.org/2005/Incubator/socialweb/XGR-socialweb-20101206/,*

[2] Open Notice Initiative Paper to W3C, Dec (2012) "Opening up the Online Notice Infrastructure An 'Open Notice' Call For Collaboration" http://www.w3.org/2012/dnt-ws/position-papers/23.pdf

[3] "World's oldest writing not poetry but a shopping receipt," by Rym Ghazal, The National, April 13, 2011, http://www.thenational.ae/news/uae-news/worlds-oldest-writing-not-poetry-but-a-shopping-receipt

[4] Evgeny Morozov, The Real Privacy Problem, MIT Technology Review, (2013). http://www.technologyreview.com/featuredstory/520426/the-real-privacy-problem/

[5] Pen America, "Chilling Effects, NSA Surveillance Drives US Writers to Self-Censor," (2013). http://www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf

[6] Search: Chilling Effects of Surveillance on Democracy. Last checked 6 June 2014: 898,000+ results. http://www.google.com/search?client=safari&rls=en&q=documented+chilling+effects+democrasy+due+to+surveillence&ie=UTF-8&oe=UTF-8#q=documented+chilling+effects+democracy+due+to+surveillance&rls=en&spell=1

[7] Open Notice Initiative Paper to W3C, Dec (2012) "Opening up the Online Notice Infrastructure An 'Open Notice' Call For Collaboration" http://www.w3.org/2012/dnt-ws/position-papers/23.pdf

[8] Chris Jay Hoofnagle & Jennifer King, *What Californians Understand about Privacy Online*, Sept. 3, 2008, available at http://ssrn.com/abstract=1262130.