# Usable Consent

Tracking and managing use of personal data with a consent transaction receipt

Mark Lizar & Mary Hodder

## Abstract

The privacy and terms of use policy infrastructure on the internet is broken.

This paper outlines a proposal for the use of an Open Notice infrastructure, for Consent Receipts, which would be created at the point of consent and used to track, manage and analyse consent on an singular and aggregated scale.

Fixing this broken aspect of digital life is a critical component to safeguarding freedom and protecting privacy for individuals as well as companies, institutions, and the democracy.

We propose creating usable public data control infrastructure to open the closed and custom format of policies with a common digital Consent Receipt standard. We hypothesise that this format, structured with the links to legally required consent notices across jurisdictions, will open the control of personal data in simple but usable way.

## Open Notice Initiative Background

Open Notice 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.[1]

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 organisations 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.

[1] 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

# 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.[2] 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, organisations 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 will require an equivalent bedrock; 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 infrastructure exploited by organisations today). 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.[3]

Agency over personal data is instrumental to autonomy, democracy and the exercise of freedoms necessary to enjoy privacy, personal data control promises to balance the trend toward 'algorithmic regulation' that big data creates with private analytics realised 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.[4]

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. 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."[5] When companies use this information beyond the stated purpose outlined in their terms of service and privacy policies or what the law allows (such as selling it to a third

[2] "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

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

[4] 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

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

party), services often act in violation of established personal, cultural and social convention. Without compliant notice, 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 limited data control compounded by the intrusion of data collection across contexts and location is threatening the autonomy of the individual in the real world and online.

Furthermore, the closed notice and data control practices are argued to have “created ‘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, imposes severe constraints on how we mature politically and socially.”[6]

# Usable Consent

People suffer from all sorts of issues that effect on the spot decision making and the quality of consent decisions.  People are notorious for making poor on the spot decisions and very much require the facilities to manage consent outside of the context it was provided.

Privacy principle, existing law and the Individual requires a framework which permits them to collect all of the privacy/security/trust assertions that are made and to store those assertions (captured in receipts) in a manner which is searchable by the individual and understandable by the party who made those promises.

Such a framework for transparency needs to be open, interoperable, inclusive and viable 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. While data controllers also require the ability to update on policy changes, further receive 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, 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; behind the 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.

Its function is to record all of the individuals consent preferences, link to required legal notice for different jurisdictions or types of data, link to the functional controls for managing the control of data and consent. For example recording consent preferences such as the Do Not Track signal in such a manner to memorialize the transaction.  Then using the link to indicate personal preferences, a personal data store or the like.

Although this receipt, available to some extent to all stakeholders, is different than a purchase receipt in that it is digital, distributed to the individual and links to a lot of data about the organisation. The individual has the choice to have a local registry of consent, as well as the option to share the Consent Receipt with the Open Notice consent registry. The consent data is distributed according to the preferences the individual sets or stores in a publically accessible place.

[6] ibid.3

Open Notice Initiative's approach will develop a distributed receipt registry for public and private use. We will do this by making open specifications, open source software and by inviting collaboration with other projects in this field. With this approach, our aim develops the basic reporting tools with 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 utilise receipts to communicate preferences and inherently make transparency more actionable.

# Scope and Interoperability

The Open Notice Initiative has 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). Rather, we will sponsor the common protocol for Consent Receipts, develop open source tools with this standard, and endeavour to facilitate, support and interoperate with many existing and emerging projects in this field.

A Consent Receipt, like a transaction receipt, is in essence a vehicle for notice information, although as a digital notice it links consent controls and channels policy information to the individual.

As 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 siloed platforms.

# Conclusion

The Open Notice & Consent Receipt approach aims to iteratively evolve the legacy consent and notice infrastructure online. It offers a specific new protocol to manage policies through a higher quality consent, which also enables a common notice infrastructure for listing privacy icons, NTIA short notices, usable terms and much more accessible privacy policies. All parties in the transaction will have a clear record of a transaction regardless of the service where consent is given through the Consent Receipt.

Ultimately, Open Notice will enable Consent Receipts to be a vehicle for delivery of choices people make, further enabling privacy icons, trust marks, and short notices to be contextualised, and interoperable. It allows for more than a single context fits all approach of the current system.