

Submitting Organization: iPrivacy LLC
Contact: Ruvan Cohen (ruvan@iprivacy.com)
Paper Name: Opting for Private Shopping
Topic: Implementing Consent/Choice
Format: MS Word
Document Name: Opting for Private Shopping.doc

Opting for Private Shopping Opting for Private Shopping: The Off-line Model Applied to On-line Transactions

**Ruvan Cohen
President, iPrivacy LLC**

As advocates on all sides of the great debate on Internet Privacy take positions regarding user consent for usage of their data, they often adopt positions that seem to ignore existing expectations of users, long established in the off-line world. The off-line methodology, while not perfect and certainly with a history of abuse, can be applied to the on-line world, despite the fact that the on-line environment ratchets up the capability of gathering and correlating a magnitude larger amount of information on users than is currently practicable in the off-line world. We will lay out the inferred principles of off-line privacy and show how they can be applied on-line. This approach forms the very basis of the development of iPrivacy's patent-pending technology and business process.

Implicit Principles of Off-line Privacy Decisions

1. The ability to complete a legal transaction is not contingent on an individual's privacy threshold.
2. There is an expectation that legal uncompleted transactions do not leave a residual PII trail.
3. There is an expectation that monitoring can be used to prevent or react to illegal transactions, but that such monitoring will be used only for tightly controlled law enforcement purposes.
4. Individuals have control over how much PII to give up for each legal completed transaction, and that control is exerted at the Point-of-Sale.
5. Release of PII is entrusted to a specific party whom the individual has:
 - a. An implicit expectation of permitted use of the PII, and
 - b. The ability to direct specific privacy guidelines.

Let's buy a pair of jeans at a bricks and mortar department store and examine the implicit privacy choices and expectations of the buyer. We will contrast these principles with some suggested approaches to on-line privacy.

Principle: The ability to complete a legal transaction is not contingent on an individual's privacy threshold.

The prospective jeans buyer makes a purchase decision first and a privacy decision at point-of-sale. To create a set of conditions in which entering into or not entering into the store is based on predetermined privacy preferences is counter intuitive and will lead to both reduced commerce and reduced privacy.

Submitting Organization: iPrivacy LLC
Contact: Ruvan Cohen (ruvan@iprivacy.com)
Paper Name: Opting for Private Shopping

The reduction in privacy will be created by buyers' frustration with their inability to complete transactions that they desire due to disembodied privacy choices.

In the on-line world, P3P creates a situation where Privacy choices and Purchase Choices are independent decisions. This could lead to the condition in which on-line customers have to choose whether they want to buy the jeans on-line and give up their privacy or not buy on-line altogether.

Principle: There is an expectation that legal uncompleted transactions do not leave a residual PII trail.

Given that the primary point of privacy decision is made at the point-of-sale, the potential jeans buyer does not assume that the style, size, or brand of jeans is recorded and added to a record on that individual, unless the consumer uses a personal shopper, whom the consumer vests with the responsibility of recording completed and uncompleted transactions. This expectation at a department store can be contrasted with the expectation of shopping at a "members only" store, at which an ID card is required for entry and purchase.

Perhaps the greatest offense to an individual's privacy expectations would be if a department store surreptitiously utilizes a "members only" identification approach. No one would feel that this would be made permissible by the posting of signs on every floor or in every department that states "we capture biometrics to enable us to serve you better." The concept of depending on conspicuously posted links to on-line privacy policies to validate surreptitious tracking methodologies and PII collection runs completely contrary to expectations.

Furthermore, to posit that all individuals who shop on-line are implicitly stating their desire to utilize a personal shopper service every time they visit a site is a violation of the shopping paradigm established in the off-line world.

Principle: There is an expectation that monitoring can be used to prevent or react to illegal transactions, but that such monitoring will be used only for tightly controlled law enforcement purposes.

The department store shopper understands the need for monitoring of activity that prevents theft. The individual is implicitly aware that security cameras monitor dressing rooms to make sure that unpaid for jeans are not concealed by baggy sweatpants. They understand that security personnel watch to make sure that unpaid for jewelry is not slipped into a thief's pocket, despite the fact that the vast majority of customers have honorable intentions. There is an acknowledged tradeoff of privacy for acceptable commercial purposes. While this expectation exists, there is also the expectation that this monitoring will not be used for other purposes for individuals with honorable intentions. There is an expectation that stores will not share security videotapes to track customer behavior store-to-store.

In the on-line world, there should be no universal expectation of anonymity. It is understandable that the department store would not appreciate the availability of devices that disabled dressing room monitoring or created invisibility. Law enforcement authorities are expected to be able to utilize due process to identify illegal activities. At the same time, there should be due process controls in place that govern this process of “illegal use” identification.

Principle: Individuals have control over how much PII to give up for each legal completed transaction, and that control is exerted at the Point-of-Sale.

Perhaps the central point for making privacy choices in the off-line world is made by individuals at the Point-of-Sale. Our jeans buyer has a number of payment alternatives that carry explicit privacy choices.

- The jeans buyer can complete their transaction using cash, providing no PII tracking capability to the department store. The store is left with an understanding of their business dynamics, but devoid of customer information.
- The jeans buyer could choose to use a general-purpose credit card, which assures funds transfer but does not provide the department store with PII. This choice explicitly provides the Credit Card Issuer with information needed for billing and settlement (merchant name, date of purchase and amount of purchase) but no information about purchase content.
- Finally, the jeans buyer can use their department store credit card, through which they are giving the department store complete control over PII and purchase content. Generally, the consumer uses this methodology of purchasing in return for value: whether it is in price, financing, service or to receive future marketing offers.

Point-of-Sale is the implicit point of privacy choice for consumers. It is a logical one, and far more nuanced than simply opt-in or opt-out. On-line consumers should have the same capability: of completing a transaction and making a decision about how much PII they wish to release in order to do so. It should be recognized that the same individual may make different privacy choices depending on the website or depending on what items they are purchasing. The transmission of PII from the consumer to the service provider is an earned privilege, not a right.

Principle: Release of PII is entrusted to a specific party whom the individual has an implicit expectation of permitted use of the PII, and the ability to direct specific privacy guidelines.

By limiting the release of PII to the payment process, the consumer has a place to focus their privacy choices and make determinations about whether the PII is being properly safeguarded. The expectation is that the credit card company will

Submitting Organization: iPrivacy LLC
Contact: Ruvan Cohen (ruvan@iprivacy.com)
Paper Name: Opting for Private Shopping

utilize the information for purposes of approving ability to pay and ability to finance. There is an understanding that they may share this information with credit bureaus for only the express purposes of refining their assessment of the individual's abilities to pay and finance. There is an implicit understanding that credit card companies will not release actual PII to unrelated third parties for marketing offers. This implicit belief has been substantiated by activities of Attorney Generals around the country, which uphold this implicit consumer desire by gaining agreement from Credit Card Companies to restrict the dissemination of PII to outside third parties, and substantiated by the recent Supreme Court's decision to disallow Credit Bureaus from selling consumer PII for marketing purposes.

iPrivacy's Approach to On-line Privacy

iPrivacy's patent pending "Private Transaction Infrastructure approach" to completing private transactions on-line effectively emulates the implicit user privacy assumptions in the off-line world in completing an on-line transaction:

1. The Credit Card Company, which until the broad adoption of on-line cash-equivalents as broadly-accepted payment mechanisms, is the only means of paying for goods and services on the internet and is the only entity (including iPrivacy) which holds any PII.
2. The Credit Card Company gets no more information than they already receive in order to facilitate payment, settlement and accurate billing.
3. All pre-sales activity and sales related correspondence is handled through a proxy server that manages cookies and sales-related electronic correspondence between buyer and seller.
4. The individual has a choice on a purchase-by-purchase basis of deciding which what PII to release to the service provider. One-time use proxy information is available to enable the individual consumer to choose whether they wish to release PII such as e-mail, name, street address, or phone number.
5. Customers can choose to login either with a proxy or public identity at any site, to receive a personalized shopping experience, without having to make that decision on a universal basis ahead of time.
6. The customer is private, not anonymous. This means that illegal activity is traceable through the Credit Card Company, but only utilizing legal due process.

iPrivacy believes that approaches that violate the individual's implicit principles of off-line privacy decisions will err either on the side of choking off on-line activity or creating a situation of broad scale privacy abuse, even through the implementation of well-intentioned programs.