

## **Online Privacy: Privacy is a good, and Keyhole Logo Proposal**

Bryan M. Griffith, 3L at The Ohio State University Moritz College of Law

Griffith.195@osu.edu

Privacy is a good which people and companies exchange for other goods and services every day. Generally privacy is the withholding of personal information manifested by choices and expectations of individuals about the sharing of their personal information. Individuals exchange bits of personal information hundreds or thousands of times per day, both online and offline. Examples of these exchanges occur when a shopper scans a frequent customer card at the grocery store, logs into amazon.com when shopping, or calls a business without blocking caller identification. Each exchange is bidirectional and individuals receive valuable goods and services, and reduced prices for those goods and services, in exchange for some personal information which in turn the business uses to improve marketing. Privacy advocates are concerned about the loss of control over this personal information, but the concern is not shared by most consumers who frequently choose to sacrifice some privacy for something of value. These consumers are placing their faith in the market to sufficiently protect their privacy. Sometimes the consumer is not given a meaningful choice, and the market incentives to protect privacy are absent—these market failures require intervention and any damages, measured by a standard value of privacy, should be borne by the wrongful party instead of the innocent consumer.

The majority of information exchanges occur transparently and the misuse is limited or prevented by the business relationship and market incentives. Transparent exchanges occur when the consumer voluntarily transmits information to another known party, usually associated with a transaction or ongoing relationship. When a consumer fills in a comment card in a restaurant with a name, phone number, and e-mail address, there is no expectation of privacy in that information and the restaurant will collect it and use that information to better market food to that person. When a computer user visits a web site and signs in with a username and password the user expects that

website to know what activities are performed while logged in at the website. These are transparent exchanges and there is no inherent expectation of privacy in these transactions.

However, some information exchanges lack transparency and may not give the user any meaningful choice. Situations which obscure the transactions include fraud, and government regulation. Fraud occurs frequently and may be the most damaging abuse of privacy. Some examples of fraudulent practices today include Nigerian 419 scams, phishing websites, and stealing confidential information from the garbage. These types of fraud lead to identity theft, and damaged credit—consumers and businesses are both hurt by this illegal activity. These actors will not comply with regulations or laws and must be addressed by technology, such as the proposed below.

Governments grant monopolies, and regulate commercial activity which may restrict competition and remove the incentive to provide offer better privacy than a competitor. These actions alter the market incentives which ordinarily give consumers the power to change a company's policy by taking their business elsewhere. Government regulation may create a false sense of security from consumers who faithfully accept the government regulation without investigating the level of protection it offers. Common carriers are regulated industries which frequently face limited competition due to regulatory constraints, or government granted monopoly. Because of the government involvement, many consumers place a great amount of faith in common carriers, and fail to investigate the privacy policies. Consumers do not have meaningful choice over which common carriers to do business with and the market may fail to incentivize them to improve consumer welfare. For these reasons, special rules have been developed to protect consumers from telephone companies who would listen to personal conversations to collect information about one's income, preferences, friends, and behaviors.

The Internet's network topology is unique amongst common carriers. During a traditional telephone call, the caller's telephone company has a direct connection to the receiver's telephone

company and at most two or three carriers are involved in the transaction. Internet transactions however are passed around ten, fifteen, or twenty times before they reach a destination, and the route may be different for every packet of information resulting in hundreds of parties having access to a given transaction. No privacy policy can control the use of the information as it is passed amongst the intermediate nodes of the Internet; only encryption technology can provide any protection against snooping internet routers. At the consumer end of the Internet, ISPs have begun to employ deep packet inspection (DPI) technology to log all Internet traffic of each user to build marketing profiles. DPI is a technology which, absent a court finding it to be an illegal wiretap, is a prime target for regulation. DPI is used by common carriers who frequently have near-monopoly power in a given market, ISPs are not adequately disclosing their use of this technology, and consumers cannot easily opt-out of the practice. Giving users a meaningful choice over the use of their personal information should acquiesce most privacy advocates, and solve the limited market failures in the realm of privacy.

A solution will address the market failure with minimal market interference. Solutions may include new technology, self-regulation, and government regulation. Meaningful choice is more nuanced than a policy mandating opt-in consent for collection would address. Forcing opt-in reveals personal information required to identify an individual for purposes of filtering that data from collection. Opt-in is a good solution where government regulation has removed meaningful choice for consumers, such as the case of DPI. For other privacy situations, an ideal solution places the filter in the hands of the consumer. Such a filter has been theorized by Eric Goldman, but Goldman's concept of a handheld history of your choices used to filter information around you is ahead of its time and the current state of portable technology.

A good intermediate solution would be to use a machine readable privacy policy and a web browser which filters content based on each site's privacy policy and the filter choices made by the user.

Today, only a few web browsers are capable of machine reading a privacy policy, but none provide meaningful choice based on the content of the policies. A good web privacy filter will be a combination of (1) a server side privacy policy in a standard machine readable format, (2) a web browser containing user privacy preferences, and (3) a simple icon to display the status of a site's privacy policy and its compliance with the user's choices. First, the machine readable policy should be embedded in the HTTP header, or located in a standard location on servers. Ideally server software companies will begin to implement an easy privacy policy editor which will automate the process. Second, the web browser must make the user's choices simple, but decisive, such as a series of yes/no questions. An example privacy practice filter might ask:

1. Do you want to view websites which collect personally identifiable information (PII)?
2. Do you want to view websites which share PII with third parties?
3. Do you want to view websites which keep PII longer than six months?
4. Do you want to view websites which do not permit you to view the data they have collected about you?
5. Do you want to view websites which collect non-PII for marketing purposes?
6. Do you want to view websites which keep non-PII for longer than six months?

Websites could voluntarily publish their answers to the same questions in their machine-readable privacy policy and the web browser would retrieve the privacy policy automatically and determine if the answers are compatible before sending the request to view other content on the server. The drawback here is that users still must send the first request to obtain the privacy policy, however that does not reveal PII or non-PII other than your IP address.

Finally, the privacy browser should display a simple logo, similar to the encryption "lock" used by most browsers to indicate websites are using SSL encryption. The logo would need to



communicate that a website complies with the user's privacy preferences. It could display three levels of compliance by changing colors showing red, meaning non-compliance, yellow, meaning partial compliance, and green, meaning full compliance. The browser would automatically show compliant websites, and prompt for permission before showing a partially compliant or non-compliant website. This would give users meaningful choice over their private information without intrusive legislation. The publication of the privacy policy also creates a contractual relationship with the user which can be enforced through a private cause of action, or an FTC § 5 action.

Privacy is a personal choice and for most users a small amount of privacy loss is well worth the cheaper goods and services received because of the exchange. Generally, users can choose to take their business elsewhere if companies violate their privacy. In those situations where government intervention has removed the users' meaningful choice, a simple regulation requiring those businesses to provide meaningful choice to customers will restore the balance of power. For the remainder of the market, a self-regulatory privacy policy scheme with a machine readable policy readable by web browsers should give users the power to make a meaningful choice without government intervention.

