

CAPITALISM AND ONLINE PRIVACY REGULATION

By: Brian Beauchamp

Introduction

Information on consumers (their location, interests, purchases, etc.) is worth a certain value to certain business entities. This information is used for directed and personalized marketing in an effort to increase consumer sales. In other words, a consumer's information is a commodity. After being categorized as such, the legal treatment of consumer information should become clearer. Like all other commodities, taking a consumer's information without consent should be impermissible. Furthermore, receiving consumer information by way of deception should be forbidden as well. In these regards, online consumer privacy should be regulated like any other industry. However, regulators should display overt caution to protect the benefits this flow of information provides to both consumers and businesses alike.

While there is a little regulation of online privacy, it is not without its mechanisms for consumer protection. With the public spotlight resting on online privacy infringements, coupled with the abundance of rivalry for online traffic, strong consumer privacy has become a competitive advantage for online companies. This has increased self-regulation and general online privacy policy standard. When these privacy policies are breached, the legislative initiatives (such as the FTC Act, The Gramm-Leach Bliley Act) provide the legal framework for enforcement. However, with technology progressing at a rapid rate, there are certain voids that are necessary to be filled with further initiatives. The following discusses ways the current laws are working, and suggestions for where they can improve.

Competition and Self-Regulation

When consumers are browsing or shopping online, the majority are not doing so blindly. News media, word-of-mouth, and other outlets have made consumers aware that online companies are interested in their information. And just like their preferences in goods sold online, consumers have their preferences to online services as well. Contemporary online companies must *compete* for a consumer's attention.

The preferences of a consumer's privacy cannot be ignored as one of these preferences. Ideally, an online illustrators must ask themselves, "how many ads can I put on this page before I pass a user's annoyance threshold?" or "how much information can I ask for, before I pass a user's suspicion threshold?" There is, indeed, a threshold.¹

With this in mind, companies have begun advertising their protection mechanisms to allay the fears of internet users. Many companies have joined self-regulating bodies to create industry standards for online privacy. Self-regulation has been described by the FTC as, "the least intrusive and most efficient means to ensure fair information practices, given the rapidly evolving nature of the Internet

¹ *Facebook Must Respect Privacy Petition*, MOVEON.ORG, Nov. 20, 2007, http://civ.moveon.org/facebookprivacy/?rc=fb_privacy. (In November of 2007, Moveon.org created an online petition for Facebook to cease its current policy for Facebook Beacon, with respect to its online privacy invasions.)

Graeme Wearden, *Privacy International Demands Yahoo Boycott*, Sep. 7, 2005, <http://news.zdnet.co.uk/internet/0,100000097,39216936,00.htm>. (In September 2005, Privacy International (PI) called on Internet users to boycott Yahoo over allegations that the Web giant provided information that helped Chinese officials convict a journalist accused of leaking state secrets.)

Sandeep Junnarkar, *Critics May Try To Widen Intel Boycott*, Feb. 16, 1999, <http://news.cnet.com/2100-1001-221672.html>. (Groups attempt to boycott Intel after news that the Pentium III processor provides the ability to trace where users have been on the internet)

and computer technology.”² Furthermore, many companies have created detailed, yet user-friendly, privacy policy statements, linked directly from their homepage, as well as opt-in/opt-out standards to comply with the Network Advertising Initiative or “NAI”.

Another independent, non-profit organization, Trust-E, has helped further online privacy goals. The company sets online standards for online privacy policy standards. Member sites have their policy standards reviewed quarterly to review compliance. Upon acceptance, Trust-E provides it Website Privacy Seal, to help consumers identify businesses with trustworthy online privacy policies.

Current Government Enforcement

Current regulation schemes have provided enforcement mechanisms for online privacy infringements. One of the most important of these mechanisms has been Section 5 of the FTC Act. Section 5 prohibits unfair and deceptive practices.³ Using the authority of this section, the Federal Trade Commission has brought a number of cases to enforce the promises in privacy statements, including promises about the security of consumers’ personal information.⁴

The Gramm-Leach-Bliley Act has also been used as an enforcement mechanism for online privacy matters. More specifically, the GLB Act includes provisions to protect consumers’ personal financial information held by financial institutions. The Act requires all financial institutions as well as institutions such as credit reporting agencies, to protect customer information.

² FTC, “*Self-Regulation and Privacy Online*,” *FTC Report to Congress*, July 13, 1999 <http://www.ftc.gov/opa/1999/07/report1999.shtm>.

³ Federal Trade Commission Act, 15 U.S.C.A. § 45 (2006).

⁴ The FTC publishes a list online of cases they enforce under Section 5 at: http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html.

With these enforcement mechanisms, the privacy promises created by online companies become legal obligations. This requires companies to follow the guidelines that competition and industry standards have imposed upon them. Over the years, however, technologies and internet activities have matured and developed. There are issues of contemporary online privacy with room for improvement.

Possible Areas for Consumer Privacy Regulation

The number of internet services provided without charge has grown exponentially over the past decade. Subscription-based internet services are losing ground, while ad-revenue sites are becoming vastly more popular. A growing number of these ads are targeted or behavioral-based advertisements. This requires consumer information in order to thrive. While the benefits (free services) are instant and highly visible, the detrimental ramifications of a consumer's actions (including the disclosure of personal information) are delayed and often inconspicuous. For these reasons, consumer protections must be in place to keep the internet a pleasurable experience. Among the issues of concern are: *Notice*, *User Consent*, and *Data Retention*.

Notice. It is of utmost importance users must be made aware of what information internet sites are extracting from them. Sites should be required to provide an easily-accessible and easily-understood privacy policy. Users cannot properly *consent* without notice of to what they are consenting. In conjunction with notice, consumer education is important as well, to provide a user the basic understanding of their rights.

User Consent. *Opt-in* requirements should be in place for all *personally identifiable information* (PII) with the ability to *opt-out* for all other types of information. There is a spectrum of value internet users place on their privacy. Thus, the amount and type of information users provide should be within their complete control.

A specific *user consent* problem that should be addressed, is the *opt-out cookie*. The same users who actively opt-out of sharing private information are the users who systematically clear their stored temporary data -- including cookies. When users wish to clear cookies that collect data, they must also clear cookies that *prevent* data from being collected; a problematic result. A possible solution is the creation of a new sort of cookie. With cooperation by both web publishers and browser developers, this cookie could be more of a “permanent” type, require a greater amount of action for deletion.

Data Retention. A notice requirement on data retention should be enacted. Furthermore, greater industry standards regarding time limitations on data retention should be ratified. The industry-specific regulation is important, as the relevance of information varies.

Conclusion

In our consumer-driven world, it should come to no surprise that information on consumers and their behaviors holds a tangible value. Because of the sensitive nature of this commodity, under-inclusive consumer protection in this area should not be an option. Equally important however, is to avoid over-inclusive and unnecessary regulation, allowing the internet to remain efficient for consumers and business alike.