

Mark Decker

I. INTRODUCTION

There are many different and frequently conflicting points of view regarding the role of government in the future of online advertising. Despite this consternation, an objective analysis of the relevant circumstances reveals that regulation of internet marketing is not only appropriate, but necessary. This paper will not presume to do the job of Congress or the Federal Trade Commission and draft the law; rather it seeks to provide an impetus for them to act. To this end, only three points need be made: 1) Internet users have a right to privacy; 2) The online advertising industry is a direct and significant threat to that privacy; and 3) The feeble self-regulatory framework concocted by the industry in the absence of meaningful government action has failed and will continue to fail to meet the privacy needs of internet users.

II. INTERNET USERS HAVE A RIGHT TO PRIVACY

Though this proposition seems self-evident, there are those in the online advertising industry who apparently feel users have no right to privacy while on the World Wide Web. Perhaps the most common iteration of this argument is that the internet is a public forum and, as such, those who enter it check their right to privacy at the door. This argument, however, has a fatal flaw: the scrutiny that can be focused on individuals by online advertisers has no ordinary counterpart in the real world. Advertisers have developed sophisticated technologies that enable them to track and observe every move a user makes on the web. The offline equivalent would be something akin to a man with camera following a person everywhere they went and recording everything they did. In other words, it would be something that would simply not be tolerated if experienced in a tangible way.

The privacy to which all users are entitled is the right to be left alone. Internet users should not be subjected to tracking and targeting just because they log on. Their data should not be constantly and unavoidably analyzed and dissected for marketing purposes. In short: commercial surveillance should not be a foregone conclusion for internet users and regulation by the government is the most expedient, efficient and effective way to achieve that goal.

III. ONLINE ADVERTISING IS A THREAT TO PERSONAL PRIVACY ONLINE

There can be little doubt that online advertising has, at the very least, the potential to be both invasive and pernicious. Reams of data are collected about individuals, many times surreptitiously, and then manipulated in ways to make them more useful to marketers, often at the expense of the privacy. In fact, many online advertisers compile digital dossiers about users by using information gathered from across the web. In turn, these dossiers could easily be paired with personally identifiable information in order to discover a user's true identity or, alternatively, they could contain such vast quantities of data that they would be de facto identifiable by virtue of their own thoroughness.

Moreover, online advertisers frequently collect data online without due regard paid to who the user is or to the potentially sensitive nature of the information being gathered. Data from a child of ten or a cancer patient researching his treatment options are subject to the same commercial exploitation as someone purchasing a mundane item. Considering the potentially sensitive nature of data advertisers may obtain in light of fact that often times that data can be traced to an individual user is incredibly distressing. The potential that it could fall (or worse, be sold) into the wrong hands is ever-present, yet the online advertising industry is either unwilling or unable to filter what information it sweeps up in its marketing dragnet.

In fact, rather than limiting the data they collect, the industry has moved toward even more comprehensive and indiscriminate online surveillance technology, the epitome of which is called “deep packet inspection” (“DPI”). DPI is nothing more than a wiretap installed by advertisers that can be used to view literally every piece of data that passes through the internet service provider. The implications cannot be overemphasized as DPI would effectively obliterate a user’s privacy on the web. More generally, DPI should serve as a warning about what online advertisers are capable of, as well as how far they are willing to go. In any event, federal regulation is necessary now in order to preserve personal privacy on the internet.

IV. SELF-REGULATION IS NOT AND WILL NOT BE ENOUGH.

The current prevailing method of controlling online advertisers is through a system of self-regulation. In other words, those with the most to gain from exploiting user data are entrusted to protect it. Disregarding the obvious flaws of such a system, a cursory glance at the framework the industry has established for itself reveals shortcomings which call into question whether online advertisers are even pretending to take self-regulation seriously. There are no meaningful oversight or enforcement mechanisms and no clear cut penalties for breaking the rules. Moreover, issues of data security and data retention are left to the discretion of the advertisers themselves so long as they are “reasonable” (and, of course, “reasonable” is never actually defined). These so-called regulations can do little to assuage the threat to privacy posed by online advertising. They are ineffective, unproductive and serve as little more than a distraction from the need for meaningful government regulation.

Furthermore, with the trend in online advertising moving inexorably toward more surveillance, the inadequacies of the current system as well the already serious privacy concerns will be magnified. The void in government leadership on this issue must come to an end.

Meaningful regulation of the online advertising industry is necessary now before the problem metastasizes.

V. CONCLUSION

The government must take a stand for consumer rights and regulate the internet marketing industry. Consumers have a right to privacy that is not being adequately protected under the current, industry-run schema and it is time for a change. There are many ways to rectify these problems: For example, shifting from an opt-out to an opt-in system and, by extension, requiring meaningful notice and informed consent would definitely be a step in the right direction. All avenues should be explored and no stone should be left unturned. The future of each American's right to privacy hangs in the balance.