

In Defense of Privacy: Protecting Consumers in an Age of Commercial Surveillance

Mark Decker
As Online Privacy Advocate Jeff Chester

I. EXECUTIVE SUMMARY

Online advertisers have strong incentives to collect and utilize as much data as possible about internet users, including potentially sensitive or intensely private information. The current self-regulatory system has failed – and will continue to fail – to provide adequate assurances of user privacy protection and data security.

Consideration of online privacy concerns in relation to internet marketing reveals serious shortcomings that must be addressed by meaningful and effective regulation, rather than the current imprecise and largely unenforceable systems whereby the industry attempts to police itself. After an examination of the types of data advertisers collect and how they use it, the threats to user privacy on the World Wide Web are apparent. The system as it currently stands is rife with potential for misuse of data; it is completely indiscriminate to who it tracks and what data it collects; and it fails to ensure that even basic levels of data security are met. Moreover, as online advertisers' technological sophistication increases, the problems already endemic in the system will become exponentially worse.

The government must step in and provide sensible rules for online advertisers that rectify the inadequacies in the current arrangement. The prevailing “opt-out” model for tracking and targeting online should be replaced by one that is “opt-in” which requires meaningful, informed consent. The definition of personally identifiable information should be expanded to include sensitive personal data such as health or financial information as well as tracking cookie data and internet protocol addresses. Moreover, this data should be rigorously protected. Finally, there

should be uniform standards to ensure that any data collected is properly secured and consumer information remains protected.

Despite the often vocal protests of industry, these simple regulations will not cripple online advertising or e-commerce (nor, by extension, the internet as a whole). The time for formal governmental intervention in the industry is now.

II. INTRODUCTION

Internet users in the United States are facing truly daunting levels of commercial surveillance. Individual privacy on the internet has eroded to the point that any or all of their activities online can be used by marketers to zero-in on them just a little more closely. The time has come for federal regulation of the online advertising industry. If internet users are to have any meaningful privacy while browsing the World Wide Web – and they should – then this step is a necessary one.

There can be no doubt that online advertising has become big business: In 2007, it generated approximately \$45 billion in revenues globally, a figure which, experts predict, will grow to \$147 billion in 2012.¹ However, as the market for online advertising continues to expand, protections necessary for an individual's privacy have lagged behind. Internet users today are subjected to a broad array of advertisement tracking and targeting technology designed to collect information about them that could be useful to a marketer.² Most troubling, perhaps, is the emergence of "behavioral marketing," wherein an advertiser builds a veritable digital dossier about a consumer and targets them specifically for certain goods and services based on

¹ Press Release, The Kelsey Group, Interactive Advertising Revenues to Reach US\$147 Billion Globally by 2012 (Feb. 25, 2008) (<http://www.kelseygroup.com/press/pr080225.asp>).

² As the Chief Marketing Officer for an online advertiser called Touch Clarity explains, its service is an "automated process of intelligent listening and responding; working with each individual visitor, based upon everything they have expressed through their click-stream interactions with you to-date. The result is significantly measured improvements in visitor engagement levels, conversion rates and most importantly, revenues." *As quoted in* BRENT HIEGELKE, IMEDIA CONNECTION, HOT STRATEGY: ON-SITE BT (Oct. 4, 2006) <http://www.imediaconnection.com/printpage/printpage.aspx?id=11474>.

information gathered by shadowing the individual as he moves about the web.³ In fact, online advertisers have compiled and maintain these dossiers in massive databases which are constantly supplemented with information gleaned from consumers as they continue to navigate the internet.⁴ Worse yet, much of the data are collected surreptitiously without the knowledge or consent of the individual being tracked.⁵ Further compounding the problems, the federal government has thus far eschewed a regulatory solution to these privacy problems in favor of allowing the online advertising community to regulate itself.⁶ Regrettably, this approach has yielded ever more intrusive and pervasive online advertising techniques while concomitantly failing to provide any adequate safeguards concerning how information about individuals online is gathered, used and stored.

With an eye toward regulation as the ultimate goal, this paper will discuss the following: First, why advertisers collect data about internet users and how they use it as well as the possible adverse consequences that could be involved for the user. Next, it will suggest areas in which the proposed regulation would need to cover in order to effectively guarantee user privacy and, finally, it will debunk several of the common arguments propounded by opponents of regulation.

III. ONLINE ADVERTISING: WHAT MARKETERS CAN COLLECT, HOW DO THEY USE IT, AND WHY IT IS A SERIOUS THREAT TO PRIVACY

³ CHANG YU, THE CLICKZ NETWORK, BEHAVIORAL MARKETING 101: DEFINING THE TERMINOLOGY (JAN. 26, 2005), <http://www.clickz.com/3463391>.

⁴ Consider, for example, the SiteCatalyst service provided a company called Omniture which states “ [w]ith Omniture, you can leverage experience gained from thousands of customers across 70 countries, including many of the industry’s online marketing leaders. Whether your company’s focus is e-commerce, email marketing, information access, rich media, mobility, optimization or even the offline channels—we can help.” Omniture “helps” by serving as a clearinghouse for consumer data collected from its many partners around the web. Available at: <http://www.omniture.com/en/partners>.

⁵ ELLEN NAKASHIMA, THE L.A. TIMES, WEB FIRMS ACKNOWLEDGE TRACKING BEHAVIOR WITHOUT CONSENT, (AUG. 12, 2008), <http://articles.latimes.com/2008/aug/12/business/fi-privacy12>.

⁶ FTC, ONLINE BEHAVIORAL ADVERTISING: MOVING THE DISCUSSION FORWARD TO POSSIBLE SELF-REGULATORY PRINCIPLES (2007), <http://www.ftc.gov/os/2007/12/P859900stmt.pdf>.

In order to understand why the regulation of online advertising is necessary, a brief overview of what information online advertisers collect, how they use it, and why it puts personal privacy at risk is instructive:

A. What Data can Online Marketers Collect?

Unfortunately for consumers, there are virtually no limits to what online advertisers can learn about them. Massive quantities of data are regularly collected by online advertising agencies. Everything from a person's name and address, to what they are searching for online and even purchases they have made in the past is there for the taking.⁷ As Gurbaksh Chahal, the founder of online advertiser BlueLithium, puts it "[t]he more we see you, the more we know about you."⁸ For example, internet advertiser ValueClick uses the data it collects across affiliated sites to determine a user's age, gender, household income, the number of children in that user's house, number of family members, level of education and even race.⁹ These demographics are in addition to information instantly available from the user's web browser including geographic location, what operating system is being used and the internet service provider among other data.¹⁰ Everything and anything done on the internet can potentially be tracked and stored by advertisers, with the result that ultimately, online advertisers are recording internet users' preferences, hopes, worries and fears, often without their consent.

B. How do Online Advertisers Use the Data they Collect?

⁷ LOUISE STORY, N.Y. TIMES, TO AIM ADS, WEB IS KEEPING CLOSER EYE ON YOU (MAR. 10, 2008), http://www.nytimes.com/2008/03/10/technology/10privacy.html?_r=1&pagewanted=print.

⁸ As quoted in Jeff Chester & Ed Mierzwinski, *Complaint and Request for Inquiry and Injunctive Relief Concerning Unfair and Deceptive Online Marketing Practices*, 9, (Nov. 1, 2006) available at: <http://www.democraticmedia.org/files/pdf/FTCadprivacy.pdf>.

⁹ VALUECLICK MEDIA, TARGETING (2008), http://www.valueclickmedia.com/adv_da_targeting.shtml.

¹⁰ *Id.*

The more information an online advertiser has about a user, the more valuable the information as a whole becomes.¹¹ Using various technologies, marketers amass tremendous amounts of data about individual consumers as they meander around World the Wide Web, assembling, piecemeal, a coherent profile of the user. In turn, these profiles are used to predict what kinds of advertisements will elicit a positive response from person associated with it.¹² Consider, for example, what online advertiser company Omniture claims its Touch Clarity behavioral advertising software is capable of:

On-site Behavioral Targeting leverages highly automated technology that takes advantage of the same web analytics data you are most likely already collecting, such as referring site, referring search engine and keyword phrase, time and day of visit, machine properties such as IP address and browser settings, along with complete individual visitor click-stream data. The system efficiently organizes the anonymous data to build individual visitor profiles containing the hundreds of data variables that occur during a visitor's visit to a web site, each with some small amount of predictive value. Highly sophisticated mathematical models then interpret these variables in real-time and assemble together their collective predictive value to determine exactly which piece of content or promotion is most likely to engage each visitor, and then serves that content while the visitor is still on the site, keeping track of the entire context of each piece of served content. The On-site Behavioral Targeting system then measures if the visitor responded to the served content in the manner predicted. By efficiently learning in real time from any differences between the predicted response behavior and actual response behavior, the system continuously makes itself smarter for the next decision.¹³

There can be little doubt that Touch Clarity is tantamount to real-time commercial surveillance of internet users and, regrettably, it is only one of many such systems deployed across the web, all with similar functions and an identical goal: learn as much as possible about the user and show them advertisements most likely to lead to a sale.¹⁴

¹¹ See TO AIM ADS, WEB IS KEEPING CLOSER EYE ON YOU, *supra* note 7.

¹² *Id.*

¹³ OMNITURE, TOUCH CLARITY: THE RISE OF ONSITE BEHAVIORAL TARGETING (MAR. 2007), <http://www.scribd.com/doc/7699893/07datasheetriseofonsitebt> .

¹⁴ See TO AIM ADS, WEB IS KEEPING CLOSER EYE ON YOU, *supra* note 7.

Online advertising advocates are quick to point out that many marketers – most notably those in the Network Advertising Initiative (“NAI”) – distinguish between information that is “personally identifiable” (for example: names, addresses or social security numbers) and information that is not (such as clickstream and demographic data).¹⁵ Armed with this distinction, online advertisers often – at their own discretion – voluntarily decline to match personally identifiable data (“PII”) with non-PII data. Therefore, or so the argument goes, all the data collected is “anonymous” because the advertisers do not know actually know the real-world identity of the user. In fact, it is based on this distinction that Omniture, as a member of the NAI, claims that the data collected by its Touch Clarity system is “anonymous.”

However, the way advertisers actually institute this practice in market suggests the data may not be so anonymous after all. According to online marketer Media Contacts, “[b]ehavioral targeting uses cookies to anonymously monitor and track users as they surf online. This information is then fused with publisher registration or survey data such as age/gender or zip/postcode. Users are then grouped or classified by content viewed, sites visited, search subjects, as well as the time, length and frequency of visits.”¹⁶ Thus, while there might not be a name or physical address attached to the online profiles of individual users that marketers are actively compiling and analyzing, unique identification numbers are assigned to each visitor instead which serve the same purpose. Online advertisers know individual user preferences, where they have gone, and what have done online. They do not need to know someone’s name to know who they are.

C. *Why is Online Advertising a Privacy Threat?*

¹⁵ NETWORK ADVERTISING INITIATIVE, FAQs (2008), <http://www.networkadvertising.org/managing/faqs.asp>.

¹⁶ As quoted in *Complaint and Request for Inquiry and Injunctive Relief Concerning Unfair and Deceptive Online Marketing Practices*, *supra* note 8 at 17.

The practice of online data collection for advertising purposes is cause for concern for many reasons. In the interests of clarity, this section will address the most serious threats to privacy individually:

1. The Potential for Misuse of Data is Inherent in the Current System

In the system as it currently stands, the guardians of the volumes of consumers' personal information collected on the internet are those that have the most to gain from exploiting it. If that seems slightly perverse, that's because it is. The NAI insists that companies are perfectly capable of preserving the anonymity of the data they collect. This despite the fact that the more information a profile contains the more valuable it becomes to the advertiser. The NAI openly acknowledges that it is a relatively simple procedure for an advertiser to combine PII and non-PII to uncover a user's real world identity if it is so inclined.¹⁷

And, in fact, online advertisers in the past *have* been so inclined. In 2000, DoubleClick, an online marketer that has since been acquired by Google, announced its intention to combine data it had collected about users with offline data obtained from a company called Abacus in an effort to personally identify users.¹⁸ Due to a massive media backlash and immense public pressure, DoubleClick ultimately backed away from its plan.¹⁹ This episode, however, still raises serious privacy concerns: What if – instead of announcing its intentions to combine the databases – DoubleClick had simply done it?

Regrettably, there is more at stake for internet users than just their anonymity. In a tragic turn of events, a woman named Amy Boyer was stalked and murdered using information – including her social security number and her place of employment – which her assailant

¹⁷ See FAQs, *supra* note 15.

¹⁸ MARK SAKALOSKY, THE CLICKZ NETWORK, DOUBLECLICK'S DOUBLE EDGE (SEPT. 3 2002), <http://www.clickz.com/1455141>.

¹⁹ *Id.*

purchased from a commercial web service.²⁰ Though extreme, Amy Boyer's story demonstrates that there can be very real consequences to having large amounts of personal data available for dissemination on the World Wide Web.

2. Online Advertising is Indiscriminate

The software programs developed by online advertisers accumulate massive quantities of information and assemble it into a coherent data that is useful to the advertiser. In doing so, however, many of these programs are indiscriminate about both whom they track and what they learn about a person.²¹ These facts carry enormous privacy implications that cannot be ignored.

Consider, for example, that an online advertising network has no idea whether a user browsing an affiliated site is an adult, a teen or a child, yet it collects and catalogues data about that user regardless. This raises the question of whether Americans are comfortable with having their children's activities on the internet constantly monitored and analyzed, even if it is for merely commercial purposes. Based on the high percentage of individuals who expressed trepidation at having their own information collected, it is likely that the answer would be a resounding "no."²²

Equally disconcerting is the prospect of an online advertising engine obtaining sensitive personal knowledge about a user and then to using it to serve advertisements that may be embarrassing or crass. User data about health or medicine, finances, and other intensely private information can easily be swept up in the internet marketing dragnet and then used to direct advertisements toward the user. A cancer patient should not have to endure being constantly shown ads related to her ailment just because she has researched her treatment options online and

²⁰ ELECTONIC PRIVACY INFORMATION CENTER, THE AMY BOYER CASE (JUN. 15, 2006), <http://www.epic.org/privacy/boyer/default.html>.

²¹ Jeff Chester & Edmund Mierzwinski, *Re: Online Behavioral Advertising Principles* (Apr. 11, 2008).

²² CONSUMERSUNION.ORG, CONSUMER REPORTS POLL: AMERICANS EXTREMELY CONCERNED ABOUT INTERNET PRIVACY (SEPT. 25, 2008), http://www.consumersunion.org/pub/core_telecom_and_utilities/006189.html

an advertiser thinks it is “relevant.” Moreover, it does not take a great leap to imagine that such information would be interesting to third parties such as health insurers or prospective employers. The fact that it is compiled creates risk that it could fall into (or be sold into) the wrong hands.

3. There are No Adequate Guarantees of Data Security

As online marketers continue to amass gargantuan databases of private consumer information, serious questions should be raised about both how that information is being protected and also how long the marketers intend to keep it. Online advertisers have no uniform system in place to ensure adequate protection of data nor is there any limit to how long data they collect can be retained.²³

More troubling, there is also agreed upon method of securing the data that is collected. The most prevalent self-regulatory model – deployed by the NAI – calls for advertisers to use “reasonable security” to protect data collected about consumers for internet marketing purposes. Reasonable security “is determined in light of several factors including, but not limited to, the sensitivity of the data, the nature of a company’s business operations, the types of risks a company faces, and the reasonable protections available to a company.”²⁴ This system invites criticism for a number of reasons.

First, consider the questions of enforcement and accountability. A review of the NAI’s most recent iteration of its self-regulatory policies, for example, reveals little in the way of how these rules will be enforced and nothing about penalties for infractions. This self-regulation scheme lacks the oversight and enforcement guarantees that a matter as significant as personal

²³ NETWORK ADVERTISING INITIATIVE, SELF-REGULATORY PRINCIPLES FOR ONLINE PREFERENCE MARKETING BY NETWORK ADVERTISERS, http://www.networkadvertising.org/pdfs/NAI_principles.pdf. Note that there is no set period of data retention advertisers agree to observe.

²⁴ *Id.*

privacy demands. Moreover, the NAI's model never actually explains what "reasonable security" even means or who makes the determination that the threshold has been met. If an online marketer believes its data security measures are reasonable only to be proven wrong when the information is stolen, it is already too late to prevent the harm from occurring.

The NAI model's problems, however, are not unique. All self-regulatory models are destined for ineffectiveness if they lack a central authority to monitor compliance. A more preferable system would involve the government (with input from the industry) establishing concrete and proven steps to ensure that marketing data is adequately protected while also requiring independent verification of that fact.

4. Online Surveillance will become more Pervasive and Invasive

Without doubt, online marketing will only become more sophisticated, more comprehensive and more prevalent. The privacy concerns mentioned above will grow as fast as the advertisers can improve their ability to track and target individuals online. Consider, for example, the concept of "deep-packet inspection."²⁵ Deep-packet inspection is an advertising technology which – when implemented at the ISP – is literally capable of seeing everything a user does online by effectively wiretapping his connection to internet.²⁶ Unfortunately, the inevitable trend for internet marketers is toward more surveillance and more information gathering; thus making more urgent the need for reasonable regulation of the online advertising industry.

IV. REASONABLE REGULATIONS ARE NECESSARY TO ENSURE USER PRIVACY ON THE WEB

As has already been noted, the call for regulation is not intended to destroy advertising on the internet. However, given the daunting privacy implications of online marketing, the

²⁵ ELECTRONIC PRIVACY INFORMATION CENTER, DEEP PACKET INSPECTION AND PRIVACY (AUG. 4, 2008), <http://epic.org/privacy/dpi>.

²⁶ *Id.*

government should not merely turn a blind eye and hope for the best. Earlier this year the Federal Trade Commission (“FTC”) sought comment on a series of principles for governing online advertising.²⁷ Though these principles are a step in the right direction, the time has come for actual regulation of the online advertising industry and not just friendly suggestions of good corporate norms and mores if consumer privacy is truly going to be protected. To that end, effective regulation will require several things:

First and foremost, the tracking and targeting of internet users should only be done if the user has given informed and meaningful consent to such practices. In other words, the current predominant “opt-out” system should be supplanted with one that is “opt-in.” Currently, in order to avoid online surveillance, an internet user has to take affirmative steps to preclude it. Rather, an opt-in system should explain to users in easy-to-understand terminology what data are being collected, how it will be used, the control the users have over it, as well as how long the advertiser will retain it and to whom it will be disclosing its findings. Moreover, any data that is collected should be effectively anonymized and only retained for a reasonable period of time thereafter.

New regulations should also make certain that personally identifiable information is broadly defined and vigorously protected. This means that the definition of PII, in addition to the commonly agreed upon ones such as full names and addresses, should be expanded to include internet protocol addresses and cookie data containing unique tracking information as well as potentially sensitive personal information such health and financial data.

Finally, policies should be implemented to ensure online advertisers establish adequate safeguards to protect the consumer data – especially PII – that may be collected. As noted

²⁷ See, ONLINE BEHAVIORAL ADVERTISING: MOVING THE DISCUSSION FORWARD TO POSSIBLE SELF-REGULATORY PRINCIPLES, *supra* note 6.

earlier, if an advertiser learns its data protection plan was unreasonable only after a breach, then it is already too late to prevent the harm. Instead, uniform guidelines should be established and independent verification that those guidelines have been met should be required.

The current system of allowing the online advertising industry to self-regulate has failed. Online tracking and targeting has grown continually more sophisticated with even more invasive technology on the horizon, users are still largely unaware they are being shadowed while they surf. Meanwhile, substantive guarantees of privacy and data security are still not available. Continued inaction by the government will inevitably lead weaker and weaker privacy for internet users.

V. SCARE TACTICS (OR WHY REGULATION WON'T DESTROY E-COMMERCE)

As noted above, online advertising is a very lucrative industry and, as such, the industry is organized and motivated to prevent any federal action it perceives as “bad for business.” Industry representatives (or those with ties to it) have numerous excuses for why the government should refrain from regulating of online advertising, wielding them like cudgels whenever the subject is broached on Capitol Hill. Though many sound plausible, these excuses do not stand up under scrutiny.

For example, a particularly popular justification for a hands-off approach by government concerning online advertising is that regulation would be bad for the economy (or would stifle the market or harm small businesses or a myriad of other related and reiterated claims).²⁸ Upon closer inspection, however, there are glaring errors in this line of argument. Recent studies have shown that many consumers in the United States are concerned about their privacy online which

²⁸ See, e.g. CHAD URBAN / PRICEWATERHOUSECOOPER'S VENTURE CAPITAL DEPARTMENT, THE ADVERSE EFFECT OF ADVERTISING LEGISLATION (NOV. 13, 2008). AVAILABLE ON TWEN.

is, experts believe, hampering the growth of e-commerce.²⁹ Consumers have made their preferences clear, a recent poll by the Consumer Reports National Research Center showed that most Americans are very concerned about what is being done with their personal information online. According to the poll:

- 82% are concerned about their credit card numbers being stolen online.
- 72% are concerned that their online behaviors are being tracked and profiled by companies.
- 93% think internet companies should always ask for permission before using personal information.
- 72% want the right to opt out when companies track their online behavior.³⁰

Federal regulation of online advertising could potentially do much to assuage consumer concerns about their privacy online and actually encourage – rather than hinder – the growth of internet commerce and the economy at large.

Moreover, if anything can be learned from the dire economic straits in which the United States currently finds itself, it is that a lack of government regulation is hardly an assurance of positive outcomes. The severity of the current economic crisis has hardly been abated by widespread deregulation of the financial markets and laissez faire economic policies; in fact, many would argue the crisis has been exacerbated by them. Trusting online marketers to protect consumer privacy going forward is as foolhardy as trusting the financial sector to police itself in hindsight.

²⁹ TAG ONLINE, ONLINE CONSUMER PRIVACY CONCERNS ARE GROWING (JAN. 7, 2007), <http://www.tagonline.org/articles.php?id=46>. Stating that “...online consumer privacy issues...are stunting the growth of e-commerce, Web marketers need to pay more attention to online privacy concerns and to give consumers more control of the personal information collected about them...”

³⁰ See CONSUMER REPORTS POLL: AMERICANS EXTREMELY CONCERNED ABOUT INTERNET PRIVACY, *supra* note 22. Stating: “‘Americans are clearly concerned with how their personal information is being collected and used by internet companies,’ said Joel Kelsey, policy analyst with Consumers Union. ‘The vast majority of consumers want more control over their personal information online and want the ability to stop internet companies from tracking and profiling them.’” Moreover, few Americans actually trust online advertising, with a recent study finding that a mere 26% of Americans said they trusted display ads.

A corollary to this argument commonly suggested by opponents of regulation is that market forces will transform the privacy issue into a competitive weapon among companies; in other words, that – if consumers truly value privacy – they will reward the companies who respect and protect it with their business, while those that do not will be driven from the marketplace.³¹ In this case, though the idealism is admirable, relying solely on the market to protect consumer privacy is just too quixotic.

It is often with good reason that the government mandates regulation: No one would argue that the Federal Aviation Administration is unnecessary because the airlines that crash most frequently will certainly go out of business. By the same token, the government should not trust individuals' privacy to be sorted out with market forces when there are potentially dreadful consequences. Moreover, with so much data collection being done behind the scenes, consumers frequently lack the information and expertise necessary to know they are even being tracked, let alone how to avoid it.³² The online utopia of perfect information necessary for this argument to hold water simply does not exist and the belief that the market itself can protect consumer privacy is romantic, but mistaken.

Finally, there are some in the online advertising business (and those who derive substantial income from it) that insist that, should the federal government begin regulating the market, then the internet would cease to exist in a recognizable form.³³ Online publishers, or so the argument goes, would be unable to extract enough revenue from regulated advertising and would have stop providing content or begin charging for it. This line of reasoning is

³¹ See, e.g. TOM BURNS / ERIC GOLDMAN, FINAL PAPER (OCT. 23, 2008) AVAILABLE ON TWEN.

³² CONSUMER REPORTS, CONSUMERS ALARMED ABOUT ONLINE PRIVACY (OCT. 3, 2008), <http://www.marketingcharts.com/interactive/consumers-alarmed-about-online-privacy-25-provide-fake-id-to-view-sites-6265>. This study shows that 48% of Americans believe – mistakenly – that their consent is necessary for information gathered about them online to be used by a company.

³³ See, e.g. MIKE TALTY / ONLINE PUBLISHERS ASSOCIATION (NOV. 13, 2008). AVAILABLE ON TWEN.

fundamentally flawed for a number of reasons. First, the internet does not exist solely as medium for commercial interaction between producers and consumers; much of the material available online is of academic or noncommercial nature. Also, with that said, there can be no dispute that internet marketing plays a vital role in the introduction and growth of valuable online content. The suggested regulations, however, are not designed to enfeeble advertising on the internet; rather it seeks only to ensure that it takes place in a responsible and transparent manner.

VII. CONCLUSION:

Internet users in the United States today are facing an era of unprecedented commercial surveillance of their day to day activities online. Many people are tracked without their knowledge, not to mention their consent, and even more invasive and, in some cases inescapable, data collection methods are looming in the near future. Privacy on the internet is quickly and quietly being stripped away by the online advertising industry and the self-regulatory scheme currently in place has only enabled this shameful state of affairs.

The government must stop deferring to the judgment of an industry that has a vested interest in harvesting as much data about as many people as is possible. Instead, it must act in favor of the public good by enforcing regulations that ensure basic levels of informed consent, privacy and security are required and maintained. Without these fundamental assurances, less scrupulous online marketers will have free reign to exploit user data without any meaningful oversight which could have dire consequences for those users in the real world. Continued inaction on the government's behalf will inexorably lead to further erosion of privacy on the World Wide Web. The time for regulation is now.