

Thoughts on the Regulation of Online Behavioral Advertising

By
Tony Frost

I. SETTING: NOT FOR NOTHING

Over the past decade and a half there has been explosive growth in consumption of the internet. Sustaining that growing use, which is most often free of direct cost to the consumer, is the aggregation of large amounts of personal data on users that is used to tailor advertisements towards them. The degree to which privacy should be protected in the world of behavioral advertising is nebulous. Promoting a balance between deregulated, free-market growth and protection of consumers from serious, specific harms due to the collection of data is the general topic of this paper. More specifically, this paper seeks to begin a conversation whereby regulatory bodies such as the FTC give consumers the tools to regulate specific harms to their privacies thereby reducing costs to government and business.

II. SOME OBSTACLES TO ENFORCEMENT OF PRIVACY RIGHTS

The biggest concern with any regulatory structure is the damage done to non-malicious actors while capturing the malicious ones. The general complaint is that a regulatory scheme will cripple a fledgling industry by reducing revenues by allowing many users to opt-out of having their data tracked thereby reducing the advertising ability of industry. Furthermore, regulation inevitably increases costs by imposing regulatory requirements on industry to protect data, exposing the companies to massive penalties in the event of innocuous breaches, and requiring compliance with onerous and rigid standards of privacy.

Severely damaging a company like Google by enacting regulations that effect their

marginal revenue and costs may seem farfetched, but regulations like these could adversely impact startup companies by forcing them to allocate their capital to the satisfaction of regulations and standards rather than towards promoting a strong product. Fundamentally, this is a concern of flexibility. We would like everyone's privacy respected, but need a stronger watchdog for some companies than for others. While Google (or AT&T or Verizon) may have the financial capability to institute more robust privacy safeguards, it has this financial advantage because it has access to more data (its revenue is tied to the amount of data it collects).

Furthermore, under less flexible regulatory approaches that require specific actions from advertisers, penalties are often not tied to specific harms. As an example, suppose a small advertiser's firewall shuts off for an hour. This is a foreseeable violation of some regulation that requires constant firewall protection of sensitive data. However, a less onerous regulatory approach would be to tie

Importantly, there is something unique about privacy in the online world – for better or worse, consumers expect that their online behavior is private. The reason that we wish to treat online advertising (and the methods of gathering data related to it) differently than offline advertising data gathering is because consumers expect their online activities to be private. However ill-founded, it seems clear that this expectation exists and should be respected, especially since the educational infrastructure to change this expectation does not currently exist. Because of this, any regulatory approach should be tailored to online activities rather than to offline data-gathering activities.

A further problem of the current approaches (including self-regulatory measures) is that while the Federal Trade Commission (FTC) has the ability to enforce promises made to

consumers by industry, it is a lumbering, cumbersome enforcer. A more agile approach might be to enable a private right to action, monitored by a sub-agency of the FTC, by those who have suffered specific harms.

III. A POSSIBLE REGULATORY STRUCTURE: CONSUMER POLICING AND LIMITED REGISTRATION

The primary goal of regulation by the FTC should be to retain flexibility in protecting consumer privacies while not placing overly burdensome regulations on business.

The major concern that I have right now is that there is no incentive to act by consumers because 1) they are unaware that their privacies are being violated (the education problem) and 2) there is nowhere to go with their complaints should they discover any. The FTC is a slow-moving entity that is unable to actively police the entire internet. But, in this area, I believe that the FTC has an advantage that it is currently overlooking. The power of the internet is its ability to spread information and connect many consumers quickly. I think the FTC should harness the power of the internet to reduce costs of registration and policing on businesses.

A possible approach would be to establish that anyone in a class of businesses¹ (those who aggregate information about consumers in order to tailor online behavioral advertisements to them) is subject to the provisions of the FTC's Act in this area. The Act could outline possible measures for storing data (based on the sensitivity of the data), transparency requirements, opt-in/opt-out requirements for specific types of online actions and so on.

In order to best police risky privacy problems the FTC could create a two-step private right of action against those violating the Act. The first step would be to file an online report with the FTC's sub agency. The agency would then decide whether or not the claim was worthy or

¹ This regulatory approach is loosely based on ideas from the Securities Acts of 1933 and 1934. The author also wishes to acknowledge that this regulatory outline is, at least in part, inspired by Professor Dale Oesterle.

frivolous and dismiss or promote it. Upon dismissal the claim could be finished, but upon promotion the filer could continue to sue the alleged breacher (step two). The advantage to this approach would be that it puts the onus on the consumer (or the legal profession) to root out bad-actors, as opposed to all businesses having to file onerous compliance reports with the FTC. This type of approach would keep businesses free from regulation until some specific harm is articulated and then approved by the agency. It also keeps the FTC from having to try to police the entire scope of business operators on the internet. There would be a significant incentive to bring meritorious claims and win them (penalties could be outlined by the FTC in the act).

A registration requirement could be triggered by the amount of data (or sensitivity of the data) collected by any particular business. If a business is dealing with large volumes (which could be defined by the FTC) then it would have to register with the FTC. This would not have to be an onerous requirement. Because the FTC would be dealing with technologically advanced businesses, it could require a simple online registration upon which the business user is directed to whatever privacy requirements the Congress or agency has enacted.

For smaller businesses that don't collect as much or any data, the FTC or its sub-agency could simply provide constructive notice that anyone dealing with the aggregation of personal information online, in order to target behavioral advertisements, falls within the class of businesses that is regulated by the FTC's Act and is therefore subject to its provisions. This approach would do two things. 1) it would appropriately delineate between the storage of information by online behavioral advertisers and credit card companies, or by other commercial outlets not tied to the internet. 2) It would appropriately protect small businesses from onerous registration requirements that might limit their abilities to perform.

Establishing a private right of action for breach of privacy would accomplish several of the FTC's goals in the regulatory area: it would establish the right to privacy on the internet as an important societal concern, it would enable self-policing by consumers (and the legal profession), and it would provide a flexible avenue for the FTC (or its sub-agency) to establish clear guidelines for industry gathering of data.

A large concern right now is that consumers don't know when their private data is being used in a violative manner. By creating a private right to sue (to be reviewed by the FTC sub agency) the FTC would only allow for penalties (in the form of lawsuits by impacted parties) based on specific harms. This type of enforcement would create an economic incentive to sue violators, which in turn provides incentive for businesses to treat private data appropriately.

An unfortunate byproduct of this type of regulation would be that businesses hide breaches more carefully, instead of being transparent about them. This is not an easily addressed problem, except to establish safe-harbor whistle-blower rules.

The goal of this type of legislation would be to side-step the debate about specific technologies (e.g. opt-in/opt-out) in order to provide large incentives to consumers to protect their own privacies and to businesses to protect data in accordance with the FTC's regulations.