OUTSELL

==========

Outsell Insights for January 7, 2013
Analysis of events, data, and trends affecting the information industry

==========

In Your Future for 2013: Navigating Tricky Privacy Waters in the USA

by David Curle, Director & Lead Analyst - Minneapolis, Minnesota

**** In a foreshadowing of what's likely to be on everybody's agenda in 2013, the FTC and members of Congress have been busy on the privacy front.***

Important Details: In the last week before the holiday season and the end-of-year wind-down, three important pieces of the privacy regulation puzzle started to fall into place:

* Data Brokers: The Federal Trade Commission, the primary US consumer protection agency, announced [1] that it had issued orders to a set of data brokers for the purposes of understanding the extent to which their products and practices threaten individual privacy. The information gathered will be used as part of the basis for future regulations. The list of companies in receipt of the orders (Acxiom, Corelogic, Datalogix, eBureau, ID Analytics, Intelius, Peekyou, Rapleaf, and Recorded Future) overlaps with, but is not identical to, the list of companies from which Senator Jay Rockefeller had earlier requested similar information (See Insights, 19 October 2012, US Senate Committee Goes After Data Brokers).

The FTC's press release explictly thanks Rockefeller and Representatives Edward Markey and Joe Barton for their input, so clearly the shadow of potential legislation hangs over the proceedings. The investigation into the data brokers is only part of a wider privacy initiative by the FTC which resulted in its important privacy report, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers [2].The orders ask for, in excruciating detail [3], information about the companies' products and practices, centering around how information is gathered, to whom it is made available, what policies are in place to protect privacy, what access consumers have to information about themselves, and what recourse they have to correct false information or to opt out of its collection or distribution.

* Childens' Privacy. The FTC also announced [4] a set of amendments to children's privacy rules under the Children's Online Privacy Protection Act (COPPA), which regulates digital products targeted at children under the age of 13, and requires parental consent for the gathering of personal information. The new rule-making strengthens existing rules, primarily by making it clear that geolocation information and photos and videos are covered as "personal information"; by closing loopholes that let plug-ins gather some information without consent; by extending COPPA to persistent identifiers (such as IP addresses and device IDs) that can persist over various websites or services; by further restricting the protections in place when operators do release information to other companies; by requiring website operators to adopt procedures for data retention and deletion; and by strengthening the FTC's oversight of "safe harbor" programs, in which certain groups of providers can opt out of the regulations by adopting a self-regulatory system.Critics have immediately jumped on a number of perceived flaws in the new rules. One line of criticism is that they shield some of the bigger tech players from liability. They target apps, for example, but with no liability for the Apple or Google app stores that sell them; and they

let Facebook off the hook [5] for contextual advertising to children as long as childrens'personal data is not used for behavioral advertising. Some complain that it's relatively easy for app providers to avoid being subject to the regulations in the first place, and others that the cost of compliance for small website and app providers will inhibit innovation.

* Cyberstalking. Senator Al Franken, who chairs the Senate Judiciary Subcommittee on Privacy, Technology and the Law, was successful in getting his subcommittee to approve a bill [6] that would prevent mobile applications from collecting geolocation information from users of smartphones and other mobile devices, or sharing it with third parties, without user consent. Franken, who has become the Senate's mobile privacy hawk, is targeting in particular a number of commercial apps that are explicitly marketed as tools for keeping track of spouses and children - and which have been used by stalkers to track and harrass women in particular. The bill is not likely to get a full hearing in this congress, but some version of this sort of protection is likely to be a part of any major privacy measures enacted in 2013.

Implications: All of these regulatory measures are attempts to deal with a persistent but complex problem that exists all across the information and technology industries: the willingness of people to trade some of their personal information for fantastic products and tools that help them in many aspects of their lives, accompanied by a growing sense of horror at how much information is actually collected about us as retail and media consumers.

The FTC is zeroing in on disclosure and opt-out policies as the way to give consumers more control in most privacy matters, but those are simple concepts that belie the devil waiting in the details. The FTC's orders [7] in the data brokers investigation should be required, sobering reading for all in the industry, because they provide an inkling of how complex a thing it is to even describe a given company's data collection practices, its privacy protections, and its relations with third parties.

Information and technology providers of all stripes will do well to begin building products from the ground up with the clear understanding that their privacy protections and data collection practices will be under constant scrutiny of the sort that's visible in the FTC's actions in 2012 - and be prepared for continued attention in 2013.

Source: Outsell Insight January 7, 2013

Outsell Inc. is a co-founder member of BIIA