Privacy Failure: U.S. Self-Regulatory Initiatives Over the Last Decade Have Left Consumers and Citizens at Risk from Expansion of Data Collection Practices

Despite a dramatic explosion in data collection in the U.S. that tracks and profiles individuals online—across all key digital platforms—there are no federal policies protecting privacy for the vast majority of Americans. With the exception of children aged 12 and under, U.S. citizens face a serious loss of privacy whenever they go online or use a mobile device. Consumer and civil liberties groups have called on Congress since the late 1990's to enact legal safeguards for privacy. Industry claims that self-regulation provides an effective safeguard have been the principal reason Congress has failed to act, leading to a decade of documented self-regulatory failure.

In 2000, the Federal Trade Commission, after extensive hearings on Internet data practices, urged Congress to pass consumer privacy legislation. Online data companies created the Network Advertising Initiative (NAI) in response, promising that its new code would protect citizens from such practices as behavioral advertising. NAI's code was supposed to limit how sensitive personal data could be used, and provide a "robust notice and choice" system for the collection of such information. In practice, the NAI proved ineffective, with few actual members and a code that was widely criticized for narrowly defining personal data and failing to address new means of tracking citizens online.

Online advertising companies, recognizing that NAI was clearly not credible, launched another self-regulatory effort in 2010. The new "Digital Advertising Alliance" (DAA), comprising the major advertising and marketing trade groups in the U.S., offered their own principles and an accompanying "icon" to inform consumers about online behavioral ads (OBA).

However, like the NAI, the DAA's definition of sensitive data permitted the collection and use of financial, health, racial, and other personal information online. Research by privacy scholars, moreover, revealed that few consumers actually understood how the DAA Principles and icon actually worked. The new self-regulatory system was criticized for only enabling a consumer to opt-out of receiving targeted ads—while their data was still processed. It also failed to provide citizens with an accurate presentation of how their information is actually used by marketers and other third parties. The NAI has joined the DAA program, and, in response to criticisms, recently proposed a revision of its own code (keeping a narrow definition of personally identifiable and sensitive data, however).

For over ten years of self-regulation, citizens have faced a pervasive and ever-expanding data collection system. Personal information is collected and compiled by tracking a consumers' use of computers, mobile phones, and gaming devices; their data profiles are stored and sold in milliseconds through invisible ad auction services; increasingly, offline and online data are merged as part of the profiling process; and social media data practices contribute a torrent of highly personal details. These developments represent an all-out assault on the privacy of the American public.