



Privacy Failure: U.S. Enforcement Actions Have Done Little to Protect Consumers From Invasive Data Collection Practices; Business Has Continued As Usual

Despite a number of high-profile enforcement efforts by both federal and state regulators industry as continued its business as usual approach of gathering massive amounts of consumers' data. At the heart of the problem is the lack of general privacy protection laws in the United States, with specific laws covering only financial information, health data and offering protection for children under 13. The Federal Trade Commission (FTC) has attempted to use its Section V authority to act against "unfair and deceptive" practices to protect users' privacy. Unfortunately companies appear to view many of the fines as merely a cost of doing business.

Take Internet giant Google for example. It has, despite various enforcement actions, emerged as serial privacy violator. When it launched its ill-fated "Buzz" social network, it revealed users' email contacts without asking their permission. The FTC reached a consent agreement that required privacy audits for 20 years. No sooner was the ink dry on the "Buzz" agreement than Google was caught hacking around privacy settings on the Safari browser, which is used on iPhones, iPads and other Apple devices. Ultimately Google agreed to pay a \$22.5 million fine, but was allowed to specifically deny wrongdoing. There was no requirement that Google delete the ill-gotten data.

And the amount of the fine is trivial to Google at only 0.045% of its annual revenue of \$50 billion. It's like a \$25 parking ticket to a person making \$50,000 a year.

Then Google was found to be surreptitiously gathering "payload data" – emails, passwords, URLs, and account numbers – from private Wi-Fi networks as its Street View cars snapped photos around the world. The FTC closed its case without taking action. A Federal Communications Commission (FCC) investigation found managers had known about the data gathering and the FCC fined Google \$25,000 for impeding its probe. The agency said it could not determine if wiretap laws had been broken because a key engineer exercised his constitutional right that he not be required to incriminate himself. Meanwhile 38 state attorneys general reached a settlement in the Wi-Spy case calling for Google to pay \$7 million and produce an public education campaign including a video explaining how to secure Wi-Fi networks.

Taken together the three fines together amount to less than one tenth of one per cent of Google's annual revenue. Thirty million dollars sounds like a lot, but it's only 0.07% of revenue. That explains why Google sees this as a minor inconvenience.

None of these this has had any real impact on Google's behavior. In 2012 it unilaterally combined privacy and data collection polices across all its services without seeking user consent. As you know, this has resulted in investigations by six European countries, but there has been no enforcement action in the United States. In its most recent privacy invasion, Google has been found to be providing personal information about consumers who buy apps from its apps store, Google Play, to apps developers in apparent violation of the "Buzz" agreement and its privacy policy. Consumer Watchdog has filed a formal complaint with the FTC, but so far there has been no enforcement action.

Simply put, enforcement actions have done little to change Google's behavior. The fines are a mere cost of doing business as they wish. And, as the leading Internet company, Google's experience with enforcement efforts sends a strong message to the rest of the industry that is simply business as usual.

#####