II-11.7: Bill to restrict online tracking currently pending before the American Congress

Lorraine Boris, Junior Editor

MAIN INFORMATION

The American Congress is currently examining a bill aiming at restricting online tracking – the Do-Not-Track-Me-Online Act. It should introduce an obligation for any online-tracking firm to allow citizens to opt-out of tracking.

CONTEXT AND SUMMARY

This bill, which was introduced to Congress on February 11th, 2011, by Jackie Speier, representative of California, is designed to strengthen the American legal framework on online tracking. It especially targets companies whose business is to collect and analyze data, and obliges them to set up an opt-out system for consumers, enabling them to configure their browser in a non-tracking mode. The bill contains several loopholes aimed at enabling companies which collect data to improve their own services to pursue their activities.

This bill comes shortly after the Federal Trade Commission (FTC), asked, in December 2010, that browser companies – mostly Google, Apple, Mozilla and Microsoft – include in their browsers an option to deactivate online tracking. This was one of the conclusions of a long-awaited report on data privacy called "Protecting Consumer Privacy in an Era of Rapid Change", and published on December 1st, 2010. Parallel to that, the FTC requested online-advertising companies to comply with these new settings.

The Do-Not-Track-Me-Online Act is more specifically designed to prevent behavioral-tracking companies from creating marketing profiles of users without their approval. These companies already do so, and most often track users on the Internet without them being given any notice. These marketing profiles are then used to specifically provide companies with the ability to develop targeted ads.

The Act states that any website with more than 15.000 visits a year – which is a wide enough scope to include most slightly successful blogs – and which uses even a basic web-analytics software – providing information such as the IP address, browser and operating system of a visitor – can face fines if no opting out option is offered to the visitor. Federal and local governmental agencies are exempted from this obligation, as well as a service such as Facebook's targeted ads. Indeed, this Act concerns companies watching people over the Internet – such as Google's DoubleClick system, not those, such as Facebook, which mainly collect the information, which internet users voluntarily give about themselves when logged in on the network.

Links with other documents in the same sector

BRIEF COMMENTARY

Currently, the FTC can impose fines on companies that have publicly agreed to offer an opt-out option and did not. Yet, it does not. Recently however, the FTC expressed its dissatisfaction with the industry's self-regulation, highlighting that the respect of data privacy has been getting laxer, at the expense of individual's rights to privacy. Indeed, information on data collection remains quite difficult to obtain for the mainstream user: even though the industry has created the Network Advertising Initiative (NAI) website, which is designed to allow internet users to opt out from online tracking, this option remains quite unknown to the vast majority of users. This NAI has been widely criticized, since it decided to work on an opt-out system that retained a narrow definition of opting out. Indeed, this could be understood as a decision to opt-out from any tracking, or to opt out from receiving targeted ads. The NAI retained a definition that does not interrupt the compilation of information on users, but merely protects them from a flow of targeted ads. On top of that, the industry failed at providing users with any tool informing them when the information is gathered, what is done with it, or enabling them to know which information is collected. In the absence of transparency, and considering the proliferation of tracking methods that vary from cookie collections to HTTP referrers and fingerprinting, the Do-Not-Track-Me-Online bill is the legal answer to this unsatisfactory self-regulation. Technically though, the Act does not specify exactly how the opt-out system should be implemented. However, it seems that Mozilla's universal header system is the easiest and most efficient system at present. Headers are pieces of information sent and received by a computer every time it acts on the Internet. It includes basic information on the browser used, the language used by the device, and the IP address. Including opting out of tracking in this header is both simple to be turned on by the user and to be read by advertising companies. It is also universal, for headers are universally used on the Internet. This system would also avoid a constant battle between protection software designers and online advertisers. This bill expresses the rising concerns over the online-tracking industry, in order to provide users access to information. As a recent case in Germany(1) showed, legislators try to set higher data protection standards for online tracking, not yet requesting transparency, but aiming at counterbalancing the asymmetry of information existing between internet users and professionals on this market. Indeed, until now, even savvy Internet users had no other option than to erase cookies on their computer to avoid being constantly tracked. No information on when, where and what information was collected was made available. This imbalance was not corrected by the industry's efforts to self-regulate. Indeed, since the online-tracking business mostly revolves around information, any favored position in the collection of the essential good on this market could hardly be dismissed by any one of the market's players, especially when no sanctions system is operative. This is a fundamental clash that is based on the place given to free will in regulatory systems. Indeed, this act claims to surpass self regulation, meaning a system organized by the industry without input from individuals, who therefore remain passive towards the system, but remains in an Anglo-American mentality that believes that it is enough that a person has expressed his consent in order for the use the system makes of his information to be completely valid. Thereby, this bill says that it is sufficient for a person to be able to opt-out of the system for the system to be entirely licit. In a more Continental interpretation, in which free will is less powerful and is not the basis of entire organizations, the State remains the guarantor of the general interest and the protection of the weak. This conception does not accept consent as a valid basis for a system to make any use it wants of a private person. Financial regulation is an example of the difference between these two interpretations. Indeed, an investor on financial markets is presumed to be a powerful person, because nobody is required to become an investor, and it is only the appetite for profit that motivates someone to speculate on the markets. Therefore, even though financial systems protected savings, no laws protected investors by treating them as though they were consumers. However, the crisis in 2008 changed this perspective, because both the Dodd-Frank Act and European legislation have described the investor as a weak person who is a potential victim of the system. Nonetheless, the Dodd-Frank Act simply requires that the person be completely informed of the risks that he or she might be directly exposed to, or indirectly exposed to because of the market's inherently risky nature. This allows us to take the measure of how much the consent of a weak party continues to be valued by the American legislature, even though the shock of the crisis has led American lawmakers to realize that consent is not a sufficiently solid basis upon which to build systemic stability, and so they have begin to address banking structures themselves via the Volker Rule.

1. See fiche Germany Google Street View