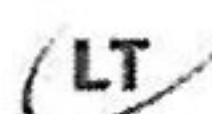


US and EU Authorities Review Privacy Threats on Social Networking Sites

TRACY GRAY, THOMAS ZEGGANE AND WINSTON MAXWELL

HOGAN & HARTSON

 Advertising; EC law; Privacy; United States; Websites

Introduction

Behavioural advertising can be defined as the tracking of a consumer's activities online in order to deliver advertising targeted to the individual consumer's interests. This practice raises privacy concerns, in particular in the context of social networking sites (SNS). Behavioural advertising is currently the subject of intense scrutiny both in the United States and in the European Union. The United States and the European Union traditionally take different approaches with regard to the protection of privacy. While the United States prefers a market-driven approach, largely centered on self-regulatory schemes supported by legislation, countries in the European Union generally apply a "top down" approach, with detailed privacy legislation based on the two EU privacy directives.¹

It is generally believed that US data subjects have a lower threshold expectation of privacy than their European counterparts. However, this analysis has been recently questioned in connection with the launch of SNS Facebook's "Beacon" programme, which has generated significant protests from users and consumer advocates.

This article will examine behavioural advertising in an SNS context to compare the United States and European Union's approaches on privacy law. The article will also assess the need to reinterpret the current regulatory framework to deal with the specific issues linked to SNS and develop consistent regulatory approaches.

What is a social networking service and how does it work?

Social networking sites are the building blocks of online social networks, used by communities of people who share interests or activities, or who are interested in exploring the interests and activities of others. Most SNS are web-based and provide a number of ways for users to interact, including chats, emails, file sharing, discussion groups and blogging. The main types of SNS are those which contain directories of categories, various means to connect with others, and "recommender" systems linked to trust, and/or a combination of these services. There are currently over 200 SNS using various networking models.

Generally, SNS allow users to create their own profiles to promote networking and a feeling of community among the participants. SNS users both provide and consume content. SNS are either closed/private communities consisting of a group of people within a company, association, society, education provider and organisation or an "invite only" group created by a user, or open/public spaces available to all web users to communicate and that may be designed to attract advertisers. Users of an SNS can be linked or become "friends" with other users. SNS generally have privacy controls that allow users to choose who can view their profiles, contact them, or be their "friends". Some social networks have additional features, such as the ability to create groups that share common interests or affiliations, upload videos and hold discussions in forums.

The more popular SNS today, including MySpace and Facebook, do not charge a membership fee, but instead, generate income through advertising revenue. The business models are increasingly based on leveraging the information about SNS users, generally found on the SNS themselves or by tracking users' individual behaviours, to provide targeted, and therefore potentially more effective, advertising.

1. Directive 95/46 dated October 24, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) and Directive 2002/58 dated July 12, 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (e-Privacy Directive) [1995] OJ L281/31.

What is Beacon and how does it work?

Beacon is a part of Facebook's advertising system that sends data from participating external websites to Facebook, as a means for facilitating targeted advertising and allowing users to share their non-Facebook activities with their friends. Facebook Beacon works through the use of a 1x1 GIF web bug on third-party websites and Facebook cookies. Clearing Facebook cookies from a user's browser or explicitly logging-off from Facebook will prevent the third-party site from knowing a Facebook user's identity. Beacon was launched on November 6, 2007 with 44 partner websites, including eBay, NYTimes.com, Hotwire, Travelocity and Blockbuster. Facebook Beacon collected data about Facebook users' non-Facebook activities, such as purchases at online retailers, reviews on other sites and auction bids, and then broadcasted this information on Facebook to their "friends" without the users' consent to do so. Furthermore, when Beacon was launched, Facebook did not announce this new service to users, and no option to opt-out of Beacon's data collection was offered.

Controversy over Beacon began almost immediately, due primarily to privacy concerns. A Facebook group and online petition demanding that Facebook not publish user activity from other websites without explicit permission from the user was circulated. Shortly after, Facebook modified Beacon to require that any actions transmitted to the Facebook site would have to be approved by the Facebook user before being published. Subsequently, users are now also able to turn off Beacon completely.

Controversy remains in that it is still unclear whether or not opting out of the Beacon programme stops third-party websites from collecting information from or providing information to Facebook.

Why are US and EU/French authorities both getting interested in Beacon?

In the United States

In today's online environment, the Federal Trade Commission (FTC) recognises that personalisation of online content (or behavioural advertising) is a major driver of internet activity and commerce. While there once was a dichotomy between first party websites and network advertisers, the shift is away from this separation, as was particularly apparent at the November 2007 FTC Town Hall meeting. In addition, the FTC's review of the Google-DoubleClick merger has further shown that behavioural tracking may raise privacy issues not only for Google-DoubleClick, but for all companies operating online.

At the FTC's Town Hall meeting, "Behavioral Advertising: Tracking, Targeting, and Technology", issues associated with behavioural advertising were discussed, prompted by the previous year's Tech-Ade hearings, petitions from consumer groups related to behavioural advertising activity, and the proposed Google-DoubleClick merger. While the FTC's definition of behavioural advertising is very broad, it has allowed the FTC to learn a lot about this type of activity both before and during the Town Hall

meeting. Currently, the FTC sees the following issues as being particularly important to focus upon and address:

- Many consumers like and value free content but do not like being tracked, do not know it is happening and are unaware of the relationship between the content they view and the information that is collected about them.
- Industry and privacy advocates alike embrace the concepts of consumer autonomy, transparency and trust.
- There is a general concern about data breaches leading to consumer data "falling into the wrong hands".
- There are concerns about the weaknesses of the Network Advertising Initiative (NAI) Self-Regulatory Principles,² including the fact that they only cover network advertisers, do not provide effective enforcement and provide an ineffective and non consumer-friendly opt-out.³

In light of the feedback received, the FTC concluded that the online advertising industry was reluctant to make any commitments or promote any behavioural advertising models. As a result, the FTC determined that the industry needs to be pushed and released the Proposed Privacy Principles as an effort to get the regulatory process started.⁴

In the EU/France

European data protection authorities are also expressing an increasing interest in SNS.⁵ The French Data Protection Authority (CNIL) announced on January 16, 2008 that it was investigating the processing of personal data by Facebook. In its press release,⁶ the CNIL expressed concerns about the risks associated with SNS's default settings, which favour an extended disclosure of personal data. The CNIL's Deputy Director for Legal Affairs also recently stated that an:

"EU working group will study the issue from February to April in order to propose recommendations for the processing of data by Social Networking Sites".

2. The NAI Self-Regulatory Principles provide specific protection for online users regarding non-personally identifiable information, data that results from the merger of personally identifiable information with non-personally identifiable information, or the combination of an internet user's name, email address or other personal information with information about their internet usage across websites, and data that results from the merger of personally identifiable information collected offline with personally identifiable information collected online for online preference marketing purposes.

3. Presentation by the FTC's Assistant Director of Privacy and Identity Protection, Jessica Rich, on February 6, 2008, in which she provided on-the-record comments on behavioural advertising and the proposed FTC Behavioural Targeting Principles.

4. See, "Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles" (FTC Proposed Principles) (FTC, 2007) <http://www.ftc.gov/os/2007/12/P859900stmt.pdf> [Accessed February 19, 2008].

5. See "Dutch DPA will focus on internet sites publishing personal data", (International Association of Privacy Professionals, 2008), *The Privacy Advisor*, p.11.

6. See "Facebook and privacy, face-to-face" (CNIL Press Release, January 16, 2008), [http://www.cnil.fr/index.php?id=2383&news\[uid\]=515&cHash=7049f4c922](http://www.cnil.fr/index.php?id=2383&news[uid]=515&cHash=7049f4c922) [Accessed February 19, 2008].

It was also stated that the CNIL intends to put the issue on the international agenda.⁷ The Chairman of the Article 29 Working Party, an independent advisory body made up of the data protection commissioners from the 27 Member States, recently stated that the Article 29 Working Party planned to investigate targeted advertising.⁸ Finally, the European Network and Information Security Agency (ENISA) issued a major report entitled, "Security Issues and Recommendations for Online Social Networks" in October 2007, putting privacy issues at the top of the agenda.⁹

How do the FTC and European authorities' positions differ?

What level of information should be given to users?

Both the FTC and European authorities are concerned that consumers are not sufficiently aware of the use that is being made of their data. As mentioned by the ENISA in its report:

"Users are often not aware of the size of the audience accessing their content. The sense of intimacy created by being among digital 'friends' often leads to inappropriate or damaging disclosures."¹⁰

The SNS environment favours extensive disclosure of data because of users' perceived sense of intimacy. This message was also highlighted by the CNIL in its recent press release regarding Facebook.¹¹

However, the collection of personal data online is not a new issue. The European e-Privacy Directive already requires full disclosure regarding the use of "cookies" to collect information relating to the behaviour of users online. Service providers are required to provide "clear and comprehensive" information about the purposes of the processing¹² and an option to refuse the use of cookies (an "opt-out" possibility). The notification and right of refusal should be offered in as "user-friendly" a manner as possible.¹³ The notification and possibility to opt-out may be given to the user once and then remain valid for the entire duration of the connection and for any subsequent connections.¹⁴

As shown by the example of Facebook's Beacon programme, the capabilities of tracking tools are greater in the SNS context

than for traditional websites. The ENISA identified the new threat linked to SNS:

"SNS provide a central repository accessible to a single provider. The high value of SNS suggests that such data is being used to considerable financial gain."¹⁵

At the same time, SNS offer new tools to control and manage the use of these tracking tools. The leading SNS provide:

"...identity-management and access-control tools for user-created content, allowing users to have control over who views their data (which is not generally permitted by blogs, for example)."¹⁶

These sophisticated tools actually enhance privacy compared to more traditional web-based services and help empower the user to control their data. In order for these tools to benefit users, they must know about them.

Both the FTC and European authorities recommend better disclosure about the risks linked to SNS and the availability of online tools to protect privacy. The main criticisms are that current disclosures are not sufficiently "clear and comprehensive"¹⁷ or "consumer-friendly".¹⁸ The FTC recommends that every website, where data is collected for behavioural advertising, provide a clear, concise, consumer-friendly and prominent statement that:

"...data about consumers' activities online is being collected at the site for use in providing advertising about products and services tailored to individual consumers' interests."¹⁹

The European Data Protection Directive already requires disclosure of information to the data subject regarding the purposes of the processing and the recipients of the data.²⁰ However, current disclosure techniques are considered insufficient by some. The ENISA recommends awareness-raising and educational campaigns on the usage of SNS, as well as contextual information within SNS to educate users in "real-time".²¹ ENISA further urges SNS to make default settings as safe as possible and accompanied by user-friendly guidelines.²² ENISA recommends that SNS publish user-friendly community guidelines rather than "terms and conditions" which are much more intimidating to users.²³

When is a consent required and in what form?

Both the FTC and European authorities want consumers to have the opportunity to disable tracking tools and be able to "opt-out." The FTC recommends that websites provide consumers with "a clear, easy-to-use, and accessible method for exercising this option."²⁴ This is similar to European law applicable to cookies: under EU law, users must be given clear information about the use of cookies and an opportunity to "opt-out." The opt-out option is not necessary with regard to:

7. See "Sur Facebook, le lecteur ne paie rien mais il peut rapporter gros", (*Marianne* 2, January 28, 2008), http://www.marianne2.fr/Facebook-dis-moi-qui-tu-es-je-ne-te-dirais-pas-a-qui-je-te-vends-_a83208.html [Accessed February 19, 2008].

8. See Maijer Palmer, "EU targets online privacy fears" (*Financial Times*, 2008). *FT.com*, February 11, 2008, http://www.ft.com/cms/s/0/8e98263a-d844-11dc-98f7-0000779fd2ac.html?ncklick_check=1 [Accessed February 19, 2008].

9. See Giles Hogben (ed.), "Security Issues and Recommendations for Online Social Networks" *ENISA Position Paper no. 1* (ENISA, October 2007) (ENISA Report).

10. ENISA Report, p.6.

11. See "Facebook and privacy, face-to-face" (CNIL Press release) stating that "users' understanding of new Social Networking Sites tools is often insufficient."

12. E-Privacy Directive Art.5(3).

13. E-Privacy Directive recital 25.

14. E-Privacy Directive recital 25.

15. ENISA Report, Threat SN.2, p.3.

16. ENISA Report, p.6.

17. E-Privacy Directive Art.5(3).

18. FTC Proposed Principles, p.3.

19. FTC Proposed Principles, p.3.

20. Data Protection Directive Art.10.

21. ENISA Report, Recommendation SN.1, p.17.

22. ENISA Report, Recommendation SN.8, p.20.

23. ENISA Report, p.17.

24. FTC Proposed Principles, p.3.

"...technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user."²⁵

This second ("strictly necessary...") exception might arguably apply to certain SNS. In addition to these two exceptions, the ePrivacy Directive indicates that service providers may make access to their website conditional on "well-informed acceptance" of a cookie or similar device, provided the cookie is used for a legitimate purpose.²⁶ Current EU privacy law permits consent to be given by:

"...any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting an Internet website."²⁷

In other words, it is possible under EU law to render the access to a service conditional on the user accepting the use of cookies.

It is unclear whether the EU legislation applicable to cookies would apply as it is to SNS tracking tools. It is clear however that in both the United States and the European Union, data protection authorities want users to provide more specific consent in connection with behavioural advertising, as opposed to consent to terms buried in the SNS' general conditions.²⁸ In the future, this may mean that users need to be given the opportunity to click a special box to "opt-out" of tracking tools.

Processing "sensitive data"

Both the FTC and European authorities²⁹ are concerned that SNS contain "sensitive data". European privacy law already defines the concept of sensitive data as:

"...personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."³⁰

The FTC's proposal is less clear, and seeks comment on what classes of information should be considered sensitive in the United States.³¹ EU privacy law submits the processing of sensitive data to higher safeguards, including express user consent and in some cases the prior authorisation of data protection authorities. The FTC is examining whether to require affirmative express consent from the user to receive advertising based on sensitive data or to prohibit such advertising entirely. The FTC mentions that in some cases consumers may appreciate receiving targeted advertising linked to (for example) health issues, provided the consumers are adequately informed in advance and clearly have a choice not to allow such processing to take place.

Data retention and data security

Both the FTC and European authorities are examining data retention practices of SNS.

The FTC recommends that data be retained only as long as is necessary to fulfill a legitimate business or law enforcement need.³² The Data Protection Directive provides that personal data must be kept in a form which permits identification of data subjects, "for no longer than is necessary for the purposes for which the data were collected."³³ The ENISA identified a threat in the SNS context linked to the difficulty of complete account deletion:

"...users wishing to delete accounts from SNS find that it is almost impossible to remove secondary information linked to their profile such as public comments on other profiles."³⁴

Some SNS platforms keep aggregate data after individual profiles have been closed. The question then is to what extent data can be rendered anonymous and kept by service providers. The way data can be rendered anonymous in turn is linked to the sensitive question of whether the internet protocol (IP) address itself is considered "personal data". As noted later in the article, the United States and Europe do not always share the same view on this question. Major SNS platforms are already responding to consumer concerns about deletion of user information. Facebook modified its help pages on February 11, and is now offering to perform a permanent deletion of an account at the user's request.³⁵ It did not however provide a one-step delete account option, noting that, "the number of users reactivating their accounts is roughly half of the number of users deactivating their accounts." An alternative could be to promote the portability of profiles, enabling the user to retrieve the information in their profile.³⁶

Both the FTC and European authorities acknowledge the importance of data security. The FTC recommends that reasonable security be provided for behavioural advertising data, based on:

"...the sensitivity of the data, the nature of a company's business operations, the types of risks a company faces, and the reasonable protections available to a company."³⁷

European privacy law requires the implementation of appropriate technical and organisational measures to protect personal data. The level of security shall be appropriate to the risks represented by the processing and the nature of the data to be protected, taking into account the state of the art and the cost of implementation.³⁸

The ENISA identified other security threats linked to SNS. First, SNS collect data which are relatively harmless individually but that can prove to be dangerous when aggregated: "profiles on

25. E-Privacy Directive Art.5(3).

26. E-Privacy Directive recital 25.

27. E-Privacy Directive recital 17.

28. ENISA Report, Recommendation SN.3, p.18:

"Descriptions of practices should be conveyed in a user-friendly way, with important information being conveyed in the context in which it is relevant, rather than being buried in Terms and Conditions."

29. See "Facebook and privacy, face-to-face" (CNIL Press release) noting that users are disclosing data relating to "habits, hobbies or even political opinions or religious views".

30. Data Protection Directive Art.10.

31. FTC Proposed Principles, p.6.

32. FTC Proposed Principles, p.4.

33. Data Protection Directive Art.6(1).

34. ENISA Report, Threat SN.6, p.3.

35. See Maria Aspen, "Quitting Facebook Gets Easier", *The New York Times*, February 13, 2008, <http://www.nytimes.com/2008/02/13/technology/13face.html?em&ex=1203051600&en=540adbdfc508f401&ei=5087%0A> [Accessed February 19, 2008].

36. ENISA Report, Recommendation SN.18, p.23 and the DataPortability and OpenID.net projects, <http://www.dataportability.org/> [Accessed February 19, 2008] and <http://openid.net/> [Accessed February 19, 2008].

37. FTC Proposed Principles, p.4.

38. Data Protection Directive Art.17.

online SNS can be downloaded and stored by third parties, creating a digital dossier of personal data."³⁹ Second, data security risks increase because of highly targeted phishing attacks, facilitated by self-created "profiles". The perceived intimacy associated with SNS also renders SNS vulnerable to:

"...social engineering techniques which exploit low entry thresholds to trust networks and to scripting attacks which allow the automated injection of phishing links."⁴⁰

Specific data breach laws are emerging in both the United States and Europe. California passed the United States' first legislation requiring notification in the event of data security breaches, which went into effect on July 1, 2003. Subsequently, at least 38 other states have followed California's lead and passed similar data breach notification laws.⁴¹ In Europe, the European Commission gave hints about its interest in implementing such measures in 2006. A proposal was formally presented by the Commission on November 13, 2007 as a modification to the European ePrivacy Directive, as well as the "Universal Service" Directive.⁴² In addition to introducing mandatory notification of security breaches resulting in users' personal data being lost or compromised, the Commission's proposal intends to strengthen security-related provisions and improve enforcement mechanisms.

Conclusion

It is anticipated that 2008 will see the emergence of new guidelines on behavioural advertising, both by the FTC and European authorities such as the Article 29 Working Group.

In addition to the issues mentioned earlier, the guidelines will have to address two key issues: (a) What constitutes personally identifiable information (PII) or personal data in an SNS context? and (b) Who is the data controller for user-generated content?

The definition of PII

The concept of personally identifiable information or personal information (collectively "PII") is troublesome. In the United States, several definitions coexist. For example, the Children's Online Privacy Protection Act of 1998 (COPPA) defines personal information as:

"...individually identifiable information about an individual collected online, including a first and last name; a home or other physical address including street name and name of a city or town; an e-mail address; a telephone number; a Social Security number; any other identifier that the Federal Trade Commission determines permits the physical or online contacting of a specific

individual; or information concerning the child or the parents of that child that the website collects online from the child and combines with an identifier described in this paragraph."⁴³

European privacy law defines "personal data" as:

"...any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."⁴⁴

In the United States, an internet protocol address is not in itself PII. An IP address only becomes PII to the extent it is associated with personally identifiable information. PII does not include information that is collected anonymously (i.e., without identification of the individual user) or demographic information not connected to an identified individual. Consequently, it is easier under US law for data collected for targeted advertising to be considered "anonymous". Under EU law, most data protection authorities take the position that IP addresses are personal data per se. In a key document,⁴⁵ the Article 29 Working Group explained that the concept of personal data is linked to the question of whether reasonable means exist to associate the data with a living person. In a majority of cases in an online environment, IP addresses can be traced to a given computer, although doing so would require the cooperation of the internet service provider and legal proceedings. Most data protection authorities consider this as sufficient for IP addresses to be considered "personal data."⁴⁶

Online tracking tools used for targeted advertising do not collect the name (or even pseudonym) of the user of the profile. In that respect, the data is anonymous. However, the IP address is involved in almost all data collection, which means that under European law, the processing would qualify as processing of "personal data." ENISA recommended that the status of IP addresses in the context of SNS be examined in more detail.⁴⁷ For global SNS platforms, it is difficult to deal with differing definitions of personal data and PII between the United States and Europe. Some form of harmonisation would be welcome.

The definition of data controller

The second area requiring clarification is the concept of "data controller" in an SNS environment. Under European privacy law, the controller is the entity which determines the purposes and

39. ENISA Report, Threat SN.1, p.3.

40. ENISA Report, Threat SN.10, p.3.

41. Luis Salazar, "Data Breach Legislation 2.0", (International Association of Privacy Professionals, January 2008) *The Privacy Advisor*, p.1.

42. Proposal 2007/0248 (COD) for a Directive "amending Directive 2002/22 on universal service and users' rights relating to electronic communications networks, Directive 2002/58 concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation 2006/2004 on consumer protection cooperation" COM/2007/0698 final.

43. Pub.L. 105-277, div C, title XIII (October 21, 1998) 112 Stat 2681-728, codified at 15 U.S.C. § 6501-6506

44. Data Protection Directive Art.2(a).

45. See "Opinion 4/2007 on the concept of personal data" (Article 29 Data Protection Working Party) http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf [Accessed February 19, 2008].

46. In France, see, CNIL, délibération 2006-294, dated December 21, 2006, Conseil d'Etat, dated May 23, 2007, 288149, Juris-Data 2007-071900, TGI Paris, Ordonnance de référé, dated December 24, 2007 (both available on <http://www.legalis.net>), TGI Saint-Brieuc, dated September 6, 2007 and TGI Bobigny, dated December 2006 (Communication Commerce électronique 12, Décembre 2007, comm. 144).

47. ENISA Report, Threat SN.2, p.8.

means of the processing of personal data.⁴⁸ In an SNS context, there are two broad categories of data: the information that the user provides to the SNS platform to register (such as the user's real name and email address), and the data that the user uploads onto his or her profile. The former is personal data which the SNS platform controls. The latter is "user generated content", which the user controls and can choose to share (or not) with others. Some SNS platforms provide the user with tools to control the extent to which information such as photos, personal tastes and the like are used to develop targeted advertising. Where such tools exist, the argument can be made that the user (and not the SNS platform itself) is the "controller" of the content the user uploads onto the profile. The concept of data controller is the cornerstone of European privacy law. The concept of controller as it is traditionally interpreted does not fit easily into the SNS environment, where the user is the focal point.

Current European privacy law may need to be clarified, in particular to specify who is the controller in an SNS environment and what constitutes personal data. This view is shared by the

ENISA which concluded that, "Legislation should be reviewed and interpreted to fit the new paradigms with which we are faced."⁴⁹

The development of international standards

The major SNS are international and want to make sure their platforms and users comply with both US and European privacy laws. Both the FTC and the Article 29 Working Party are examining the privacy aspects of targeted online advertising in an SNS environment. Both the FTC and European authorities share the same basic concerns about informing and protecting users. If the FTC and European authorities develop diverging recommendations, the compliance issues could be insurmountable for international SNS platforms, which generally cannot develop country-specific privacy options and tools. On the other hand, if the FTC and European authorities develop consistent regulations, compliance by the major SNS will be facilitated, leading to a general improvement in the level of protection for SNS users worldwide.

48. Data Protection Directive Art.2(d).

49. ENISA Report, p.25.