Privacy (regimes) Do not Threaten Location Technology Development

Bastiaan van Loenen and Jaap Zevenbergen
Delft University of Technology, the Netherlands
b.vanloenen@tudelft.nl

Abstract

Location technology allows for the tracking and tracing of individuals. Users may increasingly be concerned about the abilities of new technology to keep an eye on ones' private life. There are concerns that the increased privacy awareness among citizens and legislation may hinder the success and further development of these technologies. An analysis of the European legal framework for protecting individual's privacy versus private sector use of location information and public sector use in the intelligence services indicates that individuals should be most aware on intrusions in their privacy by intelligence services. The privacy legislation lets the user be in control of the decision if and when his location information may be used by private sector location based services providers. Users seem often willing to allow this, judging by the increase in available location based services. The privacy legislation is not as protective regarding the use for law enforcement and secret intelligence purposes. Thus the location technology industry is also likely to prosper from the investments of the public intelligence sector.

1. Introduction

Location technology allows for the tracking and tracing of individuals. Users may increasingly be concerned about the abilities of new technology to keep an eye on ones' private life. There are concerns that the increased privacy awareness among citizens and legislation may hinder the success and further development of these technologies.

In this paper, we address the concept of privacy in a general sense, discuss the European legal privacy framework for both private sector use of personal data, and use by national intelligence services. For the latter, we also summarize the framework provided by the European Court of Human Rights. Finally, we analyze the situation in the Netherlands concerning location privacy. We conclude with the implications of privacy (regimes) for the development of location technology.

2. Privacy

Privacy can be described as the right to be let alone [1]. A comprehensive description is provided by IPTS ([2], p.139): Privacy is "individuals their freedom of self-determination, their right to be different and their autonomy to engage in relationships, their freedom of choice, their autonomy as regards - for example - their sexuality, health, personality building, social appearance and behavior, and so on. It guarantees each persons uniqueness, including alternative behavior and the resistance to power at a time when it clashes with other interests or with the public interest." However, "the individual's desire for privacy is never absolute, since participation in society is an equally powerful desire" ([3], p.7).

The linkage of information to a position on the earth makes the object or subject easy to identify, easy to reach, and/ or to determine the relative position between two devices. For users of mobile devices, this may impose a serious threat to the privacy of the individual that is linked to the device. For example, the device may frequently be found at the location of a mental hospital, which may suggest that the individual has a mental problem. Conclusions drawn from this information can interfere with the daily life of the individual (see also [4]). This is especially annoying if the conclusions are inaccurate or wrong.

However, how private is location information? Danezis et al. [5] assessed the value of location information in an experiment context. They found that most participants (students) would allow their mobile phone to be queried for its location every few minutes, 24/7, for 28 days for at most (the highest bid) 30 pounds with most bids below 10 pounds. The research results suggest that location information can be acquired from 'innocent' citizens against a small monetary return. Also Westin suggests that the knowledge that one is at a certain location is less intrusive than the knowledge of what one is doing there

(see [6], 445). Further, some foresee an increasing demand for more detailed services (see [7]). Therefore, the location technology sector may not need to fear increased privacy awareness in individuals, when real value adding location based services are made available.

3. Privacy and national security

National security is an extremely flexible notion. It is difficult to define because it is closely related to subjective and sometimes emotional perceptions of administrations and military authorities about the threats to national security ([9], p.235). National security may be defined as "the universal process of surveillance by authorities to enforce the rules and taboos of society" (cf. [8], p.20). Technology allowing surveillance is increasingly important to protect national security. In order to determine a (potential) threat the use of surveillance techniques may be necessary ([8], p.22). For purposes of national security, privacy may be invaded ([9], p.1; [2], p.141).

Anyone supporting activities that are assessed to be in conflict with the norms of a society and potentially putting these norms at risk is likely to be subject to surveillance for reasons of national security.

4. Privacy legislation in Europe

The (European) Convention for the Protection of Human Rights and Fundamental Freedoms is at the core of European privacy legislation. Article 8.1 of the Convention rules that "everyone has the right to respect for his private and family life, his home and his correspondence". Article 8.2 rules that interference by a public authority with the exercise of the privacy right is prohibited except such as is *in accordance with the law* and is *necessary in a democratic society* in the interests of national security, [...].

Also the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention no. 108) requires contracting parties to implement the principles set forth by this Convention.

Further, the EU's privacy directives 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector provide the legal framework for private sector use of personal data, often including location data. Directive 2002/58/EC rules that: "[…] digital mobile networks may have the capacity to process location data which are more precise than is necessary for the transmission of communications and which are used for the provision of value added services such as services providing individualized traffic information and guidance to drivers. The processing of such data for value added services should only be allowed where subscribers have given their consent" (consideration 35). Thus, subscribers have to opt-in for use of their personal data in a location based service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data [...] which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service (art. 9).

Directive 95/46/EC (art. 28) arranges for an independent supervisory authority with effective powers to intervene in the data processing.

Since many people seem willing to give up their location privacy in return for a service benefiting them, we doubt that the opt-in requirement for location based services of the privacy legislation poses a serious threat to the use or development of location technology.

In summary, European legislation addresses location privacy, at least in theory, sufficiently for private sector use of personal data (see [10] for privacy intrusions by the private sector because of limited privacy protection in the US). However, Directive 95/46/EC does not apply to, and Directive 2002/58/EC leaves room for national governments to derogate from the directive for protecting national security interests, among others.

5. European Court of Human Rights

The European Court of Human Rights (ECHR) oversees the implementation of the (European) Convention for the Protection of Human Rights and Fundamental Freedoms. In its' rulings the ECHR has developed upon the requirements 'in accordance with the law' and 'necessary in a democratic society'.

5.1. In accordance with the law

In the Court's settled case-law, "in accordance with the law" not only requires the impugned measure to have some basis in domestic law, but also refers to the quality of the law in question: it should be accessible to the person concerned and foreseeable as to its effects (see *Rotaru*, §52). The law must be compatible with the rule of law; it must provide effective remedies against arbitrary interference by public authorities with the privacy rights of Article 8. Article 13 of the

Convention requires that these remedies are "effective" in practice as well as in law (*Rotaru* §67).

Especially interference with an individual his rights through secret surveillance by intelligence services, should be subject to an effective control. This control should normally be assured by the judiciary, at least in the last resort, since judicial control offers the best guarantees of independence, impartiality and a proper procedure (*Klass*, §§55-56; *Segerstedt* §76; *Leander*, §50; *Malone*, §67). The "authority" may not necessarily in all instances be a judicial authority in the strict sense. But the powers and procedural guarantees the authority possesses are relevant in determining whether the remedy is effective (*Rotaru* §69; *Segerstedt* §117).

In a recent case, the ECHR found the German remedy for ubiquitous monitoring of satellite telephone conversations effective (*Weber*, §152-156). The Federal Minister is empowered for deciding on the use of intrusive means by the Federal or state prime minister. The independent Parliamentary Supervisory Board –consisting of members of parliament, including members of the opposition– needs to be informed at least every six months about the implementation of the law. Further, the independent Supervisory Commission has to authorize surveillance measures and has substantial power in relation to all stages of interception (*Weber*, §§117,24; cf. *Segerstedt* §118).

Moreover, monitoring needs to be discontinued immediately once the conditions set out in the monitoring order are no longer fulfilled or the measures themselves are no longer necessary (*Weber*, §116).

We may conclude that effective remedy requires that the authority carrying out the control needs to be sufficiently independent (preferably with representatives of parliament including the opposition), and vested with sufficient powers and competence to exercise an effective and continuous control (cf. *Klass*, §56). Sufficient powers are the power to render legally binding decisions in all stages of the surveillance process.

5.2. Necessary in a democratic society

The ECHR has ruled that in order for intrusive means to be considered necessary in a democratic society several issues need to be addressed.

5.2.1. A fair balance has to be struck between the demands of the general interest and the interest of the individual. The Court must determine whether a fair balance was struck between the demands of the general interest of the community and the requirements of the protection of the individual's fundamental rights. ECHR has ruled that "the mere fact that 'information' or 'ideas' offend, shock or disturb does not suffice to justify that interference [...]". However, actions that offend the values of a society and incite to violence to change these values justify measures to protect national security ([9], p. 338; see also *Sürek* § 40).

5.2.2. Interference should be proportionate to the legitimate aim pursued. According to the Court's settled case law, a legitimate aim needs to be pursued, and there should be a "reasonable relationship of proportionality between the means employed and the aim sought to be realised" (*Marckx* §33; *Dudgeon*, §53). If the aim sought can be realized with alternative less intrusive means, the ECHR finds the intrusion disproportionate (*Olsson*, §83; *Hatton*, §97).

However, national security needs do not automatically prevail. In *Klass* the ECHR affirms that the danger of a law allowing secret surveillance poses a threat of undermining or even destroying democracy on the ground of defending it. Therefore, the countries may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate (*Klass*, § 49).

5.2.3. Interference is only allowed if adequate and effective guarantees against abuse exist. In the context of secret measures of surveillance or interception of communications by public authorities, because of the lack of public scrutiny and the risk of misuse of power, the domestic law must provide some protection to the individual against arbitrary interference with Article 8 rights (*Malone*, §67). The court has ruled that interference can only be regarded as "necessary in a democratic society" if the particular system of secret surveillance adopted contains adequate guarantees against abuse (*Malone*, §§ 49-50) (see 5.1).

6. Location privacy in the Netherlands

6.1. Adequate and effective guarantees against abuse: who decides on surveillance?

In the Netherlands, it depends on the intrusiveness of the means that are utilized who balances the general interest with the interest of the individual. For most means, the responsible Minister of the Interior, or the head of the intelligence service has to decide on the interference. For (e-) surveillance the Minister of Interior needs to consent. There is no independent supervision over this decision.

Presently, concerning the location data of terminal equipment, the Dutch intelligence services are only

allowed to request data that are directly related to the use of the equipment. Location data can only be used for tracking if the user communicates 'actively' (like making a phone call or sending a text message). It is explicitly prohibited to trace a person on a continuous basis through the stand-by mode of his cell-phone (Nota van toelichting Besluit ex artikel 28 WIV 2002).

6.2. Adequate and effective guarantees against abuse: remedies for citizens

The independent Supervisory Commission assesses ex-post the legitimacy of the acts of the national intelligence service and advises the Minister on security issues. The Commission must be provided with all information that it thinks are necessary for the adequate execution of its' tasks. The Commission reports on its findings. However, the Commission cannot render any legally binding decision.

Further, parliament has enacted a Commission for the Intelligence and Security Services with political leaders of most political parties. This Commission discusses in strict secrecy the operational activities of the intelligent services. The intelligence service sends a yearly report of the service to the national parliament.

Any complaints should be filed with the National Ombudsman. Before submitting a claim, the concerning Minister is notified about this intention. The Minister provides his point of view after consultation with the Supervisory Commission. If the Minister's point of view does not satisfy the 'plaintiff', the complaint may be submitted to the National Ombudsman. The Ombudsman can access secret files of the intelligence service, on the condition that the content of the files remains secret. He judges the complaint and his statement may be accompanied with recommendations for the national intelligence service. The Ombudsman cannot render legally binding decisions.

It has been suggested that citizens may ultimately file a suit under civil law. The civil judge, however, does not have and cannot require full access to the information of the secret intelligence services. It may therefore judge on the basis of insufficient information. Recently, the Supervisory Commission responded to a civil court's ruling, which it found unjust basing itself on secret information that was inaccessible to the judge (see [11]).

We conclude that it is unlikely that the present Dutch remedy would pass as effective when a case would be brought before the ECHR (cf.. [12], p. 833; [13], p. 46)

6.3. Recent developments towards increased surveillance

Recent developments are pressing the balance between privacy and national security towards national security (see [14], p. 18-19). For example, since 1 July 2005, providers of telecommunication networks and services are required to provide the intelligence services on request with data concerning a user and the telecommunication traffic with regard to this user. Since 1 February 2007, law enforcement agencies can apply special powers if there is a probable cause for terrorism or other severe criminal acts. This is a lighter requirement than the previous required reasonable suspicion. In May 2006, new legislation was proposed requiring organizations responsible for financial services (banks, credit card companies, credit organizations) or those operating as a provider of traffic services (airports, airlines, ferries, public transportation, etc.) to provide on request data to the intelligence services (article 29a, Kamerstukken 30553). This bill is still under discussion.

In line with these developments, it is conceivable that in the near future a situation will emerge where the national intelligence services will be allowed to track a person continuously even if the cell phone is in the standby mode or turned 'off'.

7. Conclusion

It remains a question how private location information is. The fact that it is known that one is at a certain location is not as intrusive as some may think. Consequently, the location technology sector may not need to fear as much the privacy awareness of individuals. The individual user is in control of his location data, but as long as a location based services provider supplies services desired by the user, the European privacy legislation does not limit the private sector use of location technology.

For privacy protection against invasion by secret intelligence services, European citizens rely on the European Court of Human Rights. According to the Court's judgments effective remedies should be available to protect citizens against arbitrary interference with their privacy. We may conclude that effective remedy requires that the authority carrying out the control needs to be sufficiently independent (preferably with representatives of parliament including the opposition), and vested with powers to render legally binding decisions in all stages of the surveillance process. In the Netherlands it is doubtful whether in case of use for purposes of national security, citizens have these guarantees and legal

means to protect their privacy. Secret surveillance is increasingly allowed, including location tracking and tracing.

Although certain people may be concerned with both the use in private sector (see [10]) and the developments in national security, Europe seems to provide a reasonably balanced legal privacy framework that leaves ample opportunities for the location technology industry, both for value adding location based services, as well as for secret surveillance by the authorities.

8. Acknowledgements

This ongoing research has been accomplished under research grant 458-04-022 from the NWO program Netwerk voor Netwerken.

9. References

[1] T. Cooley, "Cooley on Torts 2d ed.", p. 29, 1880.

[2] IPTS (Institute for Prospective Technological Studies), "Security and privacy for the citizen in the post-September 11 digital age: A prospective overview," Report to the European Parliament Committee on Citizens Freedoms and Rights, Justice and Home affairs (LIBE) 2003.

[3] A. F. Westin, *Privacy and Freedom*. New York: Atheneum, 1967.

[4] M. Gruteser and D. Grunwald, "A methodological assessment of location privacy risks in wireless hotspot networks," *Lecture notes in computer science*, vol. 2802, pp. 10-24, 2004.

[5] G. Danezis, Stephen Lewis, and R. Anderson, "How much is your privacy worth?" *Fourth Workshop on the Economics of Information Security*, 2005.

[6] A. F. Westin, "Social and political dimensions of privacy," *Journal of Social Issues*, vol. 59, pp. 431-453, 2003.

[7] J. Smith and A. Kealy, "SDI and Location Based Wireless Applications," in *Developing Spatial Data Infrastructures: From Concept to Reality*, I. Williamson, A. Rajabifard, and M.-E. F. Feeney, Eds. London: Taylor and Francis, 2003, pp. 263-279.

[8] G. T. Marx, "What's new about the "new surveillance"? Classifying for change and continuity," *Surveillance and Society*, vol. 1, pp. 9-29, 2002.

[9] J. P. Loof, *Mensenrechten en staatsveiligheid: verenigbare grootheden?* Wolf Legal Publishers, 2005.

[10] R. O'Harrow Jr., *No place to hide; Behind the scenes of our emerging surveillance society*: The Free Press, 2005.

[11] Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten, "Toezichtsrapport inzake het onderzoek van de AIVD naar het uitlekken van staatsgehei-men (rapportnr. 10)," November 2006.

[12] J. P. Loof, "Noot 89," *European Human Rights Cases*, vol. 7, pp. 818-833, 2006.

[13] Raad voor het openbaar bestuur, "Tussen oor-log en vrede; Kader voor een balans tussen vrijheidsrechten en veiligheid," oktober 2005.

[14] B. J. Koops, *Tendensen in opsporing en technologie; Over twee honden en een kalf*: Wolf Legal Publishers, 2006.

European Court of Human Rights judgments

Dudgeon v. UK, (appl. no. 7525/76), 22 October 1981
Hatton and Others v. UK (no.1), (appl. no. 36022/97 2003), 2 October 2001
Klass and Others v. Germany, (appl. no. 5029/71), 6 September 1978
Leander v. Sweden (appl. no. 9248/81), 26 March 1987
Malone v. UK, (appl. no. 8691/79), 2 August 1984
Marckx v. Belgium, (appl. no. 6833/74), 13 June 1979
Olsson v. Sweden (no.1), (appl. no. 10465/83), 24 March 1988
Rotaru v. Romania, (appl. no. 28341/95), 4 May 2000
Segerstedt-Wiberg and others v. Sweden, (appl. no. 62332/00), 6 June 2006
Sürek v. Turkey (no. 3), (appl. no. 24735/94), 8 July 1999
Weber and Savaria v. Germany, third section decision as to the admissibility of appl. no. 54934/00, 29 June 2006