UACES 47th Annual Conference

Krakow, 4-6 September 2017

www.uaces.org

Hartmut Aden and Johanna Schmidt-Bens, Berlin School of Economics and Law

Tracking Technology, Privacy and Accountability: Regulatory Challenges in the EU[1]

Paper for the UACES 47th Annual Conference, Jagiellonian University, Krakow, Poland,

4-6 September 2017, panel 811 on "Justice and Home Affairs in the Fading EU"

[Draft – please do not quote without the authors' permission. Critique and comments are very welcome.]

© + contact details corresponding author:

Prof. Dr. Hartmut Aden
Professor of European and German Public Law, Public Policy and Public Administration
Hochschule für Wirtschaft und Recht Berlin/
Berlin School of Economics and Law
Department of Police and Security Management
Deputy Director, Forschungsinstitut für Öffentliche und Private Sicherheit/Berlin Institute for Safety and Security Research (FÖPS Berlin)
Alt-Friedrichsfelde 60
D-10315 Berlin

E-Mail: Hartmut.Aden@hwr-berlin.de
Website: www.hwr-berlin.de/prof/hartmut-aden
http://www.foeps-berlin.org/

[1] This paper is related to the research project "FindMyBike - Rechtliche und technische Konzepte für die Übertragung von zeitbasierten Geodaten zur Aufklärung von Fahrraddiebstählen" that has started in April 2017. The authors would like to thank the *Institut für Angewandte Forschung* (IFAF) Berlin for funding this project. The co-author Prof. Dr. Hartmut Aden is co-directing this research project with Prof. Dr. Gudrun Görlitz (Beuth Hochschule Berlin), the co-author Dr. Johanna Schmidt-Bens is senior research assistant in this project. We would also like to thank Mr. Alexander Vollmar for his helpful comments related to the technological aspects of this paper.

Abstract

Tracking technologies, mostly based on the Global Positioning System (GPS), make the local position of a device visible for the users and for others who have access to the data. The widespread use of mobile devices connected to the internet, e.g. smart phones and tablet computers, has massively expanded the number of applications based on GPS. Many applications not only facilitate the users' orientation, but also track where the device and its user have been in the past.

The use of tracking technology therefore produces data that has become interesting for big data analysts for marketing purposes, e.g. in order to learn how customers move in shops and shopping malls. Secret services and law enforcement agencies are also interested in having access to this data, for example in order to know where a person suspected to have been involved in terrorist attacks or to have committed a crime has been in a relevant period of time.

Therefore, the use of tracking technology leads to the question of how privacy, data protection and accountability can be adequately taken into account for the use of tracking data. The paper asks which national, European supranational and international regulatory approaches can be developed to limit the use of tracking data to cases of serious security threats, while protecting individuals against the misuse of tracking data for surveillance purposes by private actors and state agencies. It is based on the hypothesis that "classical" regulation (i.e. by law) and technological solutions should be combined in order to adequately protect the individuals' rights when they use tracking technologies.

Key words: Tracking technology; geo-location; Global Positioning System (GPS); police cooperation; surveillance; Area of Freedom Security and Justice; data protection

1. Introduction

Surveillance is closely related to technology. In many cases, the European Union has supported technology that can be used for surveillance purposes, often by funding related research. With the Treaty of Lisbon, the Charter of Fundamental Rights became binding, and the EU gained new law-making powers for the security field. Therefore, the EU has assumed increased responsibility for protecting the citizens' fundamental rights against surveillance. This paper analyses the tensions between surveillance and fundamental rights for the use of geo-location tracking technology.

The use of geo-location tracking technology is based on satellite navigation. A satellite navigation system with global coverage is called a global navigation satellite system (GNSS). This term covers different systems as the United States (U.S.) *Global Positioning System* (GPS), the Russian *Global Navigation Satellite System* (GLONASS), the European alternative called the *Galileo Positioning System* (expected to be in use in 2020) and the Chinese System *Beidou*. In 2004, the EU established the *European GNSS Agency* in order to promote the development of geo-location technology in Europe.[2]

The GPS has been in development since the 1970s, and was initially designed for US military purposes. A network of satellites makes it possible to locate the position of a device using GPS technology. Beyond the use of this system for military purposes, GPS has become predominant in numerous applications using satellite-based geo-location. Since the daily use of smartphones and tablet computers has become the norm for people worldwide, the practical relevance of GPS has increased considerably. European initiatives to establish Galileo as an alternative system have not yet challenged the predominance of the GPS. However, GPS geo-location has not only led to useful applications for consumers, but also to new forms of surveillance.

This paper analyses from a trans-disciplinary legal and political science perspective the ambiguous effects of geo-location tracking and the regulatory challenges that result from this ambiguity. The paper more specifically looks at the European Union (EU) with its ambiguous role as facilitator and regulator of tracking technology. The sometimes difficult distinction between useful applications and problematic surveillance leads to regulatory challenges for the use of geo-location tracking by private actors and by public authorities, which is to be

[2] Based on Regulation (EU) No. 912/2010, JO EU L 276 of 20.10.2010, p. 13, amended by Regulation (EU) No. 512/2014 of 16 April 2014, JO EU L 150 of 20.5.2014, p. 72.

discussed in the following sections of this paper. Three research questions are guiding the analysis. (1) What is the role of the EU as facilitator and regulator for the use of tracking technology for the private and the public sector? (2) Which regulatory approaches can be developed within the EU, at national and international levels in order to protect individuals against the misuse of tracking data for surveillance purposes by private actors and state agencies? (3) And how can private actors and public security agencies be held accountable for how they make use of tracking data? The analysis is based on the hypothesis that "classical" regulation (i.e. by law) and technological solutions should be combined in order to effectively and adequately protect individuals' rights when using tracking technologies.

2. How does geo-location tracking work?

Using geo-location technology for tracking purposes requires technically specific devices. A network of satellites is the key element of geo-location. These satellites cover the entire surface of the Earth, orbiting at an altitude of approximately 20.000 km. The satellites are capable of measuring the distance to a device used on the ground. The relevant distance data to at least three of the geo-location satellites is necessary to calculate the position of the device. With more satellites involved, the geo-location will become even more precise.

Geo-location works in combination with software applications on users' devices. Smart phones and tablet computers have become widespread technologies since 2007 when Apple launched the iPhone. Since then, the use of applications based on geo-location has become an important element of everyday life. Applications generally request the user's consent to process his or her position data. However, what private actors and security agencies do with this data is usually not as transparent. The users are in fact limited in their control over to whom exactly, how, and for what purposes their geo-location data is transmitted.

Along with the applications that people use on their smart phones and tablet computers, geo-location is also related to the internet. Many applications using geo-location are internet-based, as is the data processing that follows the collection of position data. Geo-location can also be based on wireless internet connections (Wi-Fi) for devices connected to Wi-Fi networks. The growing importance of Wi-Fi offered for free by bars, hotels, shops, public transport, etc. has therefore opened new technological options for geo-location and surveillance that may be combined with satellite-based tracking.

3. Useful applications and surveillance

Geo-location enables useful applications facilitating everyday life, but it also creates new options for surveillance. The two sides co-exist, with difficulty sometimes arising in simply classifying an application as one or the other. This makes regulation a challenge. The EU has supported both with initiatives for enhanced research on geo-location.

3.1 Useful applications in everyday life and for professionals

On the one hand, geo-location has become a tool that makes useful information easily available. Numerous applications on mobile devices therefore use geo-location.

Geo-location based navigation is the most widespread of these applications. It continues to go further and further in replacing traditional printed maps. These applications make it easy to find shops and services in local surroundings, for example a hotel or a good restaurant. Feedback and rating systems lend more character to these applications than simple commercial advertising.

Not only have individuals discovered useful applications made possible by geo-location and position tracking, but public administrations, research institutes and non-governmental organisations (NGOs) have found the same. Researchers use geo-location for activities like tracking the movements of wild animals for scientific or preservation purposes. Car-sharing and bicycle rentals use geo-location technology to track their vehicles. The convenience of allowing customers to leave bicycles anywhere within a predefined area could only be made possible by tracking technology, allowing the bicycles to be detected and collected efficiently.

Many of these applications not only use the current position of a device, but also store data on its previous positions. This makes possible an ex-post documentation of the movements that a device and the person(s) who carried it have made. Users may find this useful, e.g. athletes wishing to evaluate their running or cycling performance. In the case that an asset equipped with geo-location gets lost or stolen, tracking technology may facilitate finding it.

Geo-location can also be used by the public sector, e.g. for tracking the position of buses and trams, police cars or ambulances. This may facilitate the coordination of these kinds of services and help expedite their journeys to the places where they are needed.

3.2 Undesired surveillance – more than a side-effect

On the other hand, geo-location can be used for surveillance purposes. The individuals concerned would in many cases not agree to the surveillance if they were fully aware of this occurrence. The previous examples have already demonstrated that some applications may be ambiguous: For example, data storage on past movements may be useful for some people, while for others, knowing that all this data is collected and stored may be frightening and perceived as an encroachment on privacy. In this respect, the use of geo-location is part of the broader debate on the use of mass surveillance (cf. Cohen 2014; Landau 2010; Lyon 2015).

For private actors, using GPS data for surveillance purposes has become interesting – not only for reasons of individual curiosity or for private investigators, but also for commercial purposes. Specific applications are able to track the movements of customers in a shop or in a shopping mall with the help of the customer's smart phone. This data can then be used for marketing purposes, e.g. in order to find out where a product should be placed in a shop. So far, customers have been left unaware of this tracking, not having ever been asked to give consent for this kind of data retention.

Public law enforcement and intelligence services may use tracking data for the surveillance of individuals. The retention of meta-data on citizens' communication makes it possible to track where an individual's electronic device has been during the retention period. For police investigators or intelligence services this data may contain interesting information, for example indicating connections to other crimes or criminal networks. Security agencies can also use geo-location for secret observation by placing a geo-location transmitter in a vehicle used by a targeted individual.

4. The EU as enabler of tracking technologies

The EU can be described as an enabler for the development of new tracking technologies as well as a facilitator for geo-location based surveillance mechanisms. As a consequence, the EU is playing an ambiguous role in that context.

The implementation of the European satellite navigation system Galileo demonstrates that ambiguity. Galileo is a core element of the current European space strategy. According to the

Galileo Regulation[3], one of the goals defined for the Galileo programme is to mobilise the economic and strategic advantages of having European control over the continuous availability of satellite navigation services. The Regulation also promotes the development of new products and services based on satellite signals. Galileo has been expressively designed for civilian purposes, for example to support the navigation in (connected) cars as well as to improve transportation, road safety, telecommunications, agriculture, or energy supply (Recital 2). It has also been stated that public authorities may benefit from these systems in various areas such as emergency services, police, crisis management or border management (Recital 8). They may use the future European geo-location technology for organising and facilitating their own work, but also for surveillance purposes.

The promotion of the EU's Galileo programme shows that technology is never neutral. Even if a new technology is intended to promote the development of new products facilitating everyday life and assuring future economic growth, it can also be used for developing new surveillance strategies. Therefore the regulatory framework and the accountability for the development as well as the use of tracking technology remain major issues.

5. Challenges of regulating geo-location at transnational or EU level

As tracking data can be linked to a particular individual, data privacy laws have to be respected. With regard to the fast-paced development and use of new tracking technology, its regulation must be continuously reviewed and adapted. The following section discusses, from a trans-disciplinary legal and political science perspective, challenges for the regulation of geo-location tracking.

5.1 Regulatory challenges related to transnational data processing

The transnational character of technology is particularly challenging for regulating the use of geo-location data. Regulation only follows more traditional paths if the companies or institutions using tracking data are based in the same country as the individuals whose data is used for tracking. This, for example, is the case for criminal investigation, which is still mainly regulated by national criminal procedure. In Council of Europe countries, judgments by the European Court of Human Rights lead to some common minimum standards. Beyond

[3] Regulation (EU) No 1285/2013 of the European parliament and of the Council of 11 December 2013 on the implementation and exploitation of European satellite navigation systems and repealing Council Regulation (EC) No 876/2002 and Regulation (EC) No 683/2008 of the European Parliament and of the Council.

this harmonisation by case law the extent to which encroachments upon fundamental rights are allowed will be monitored only by domestic institutions.

However, when intelligence services retain data on individual communication in other countries, or when police or intelligence services share tracking data with colleagues from abroad, regulation tends to become more complicated. Domestic law will then either not be applicable, or be unable to limit the foreign security agencies' activities effectively. Beyond Europe, transnational regulation of data processing is still fragmented and for many areas non-existent.

5.2 The EU as regulator of tracking technologies for commercial purposes?

Legal rules regarding the use of tracking technology by private actors for commercial purposes must mediate the conflict between the commercial entities' interest in the analysis of personal data, and individuals' rights to privacy.

Regulation may take several approaches. State interventions prohibiting certain types of data collecting might be one possible approach. However, in view of the commercial interest to use the customers' data, this far-reaching regulatory approach will be attacked by the relevant lobby groups and therefore difficult to achieve. Another regulatory approach consists of forcing private actors to at least make the collection of tracking data transparent for their customers. Only if customers know about data collection, will they have a chance to decide if they want to use an application that tracks their movements.

The EU legislation on privacy and digitalisation demonstrates the challenges of finding a compromise in this field. In 2010 the European Commission set up a *Digital Agenda for Europe* (European Commission 2010) with the overall aim to deliver sustainable economic and social benefits from a digital single market. To reach that goal, the Commission identified building digital confidence and enhancing trust and security as significant factors. It stated that a lack of the users' trust in the online environment would hamper the development of Europe's online economy. Users feeling safe and secure when connecting online were seen as a necessary precondition for embracing new technology (European Commission 2010, sections 2.1.3 and 2.3). The Digital Agenda highlighted the enforcement of the right to privacy and to the protection of personal data as guaranteed be the Charter of Fundamental rights, promoting strategies such as enhancing the application of "Privacy by Design" or increasing the responsibilities of network operators and service providers.

The *Digital Single Market Strategy (DSM Strategy)* published by the Commission in 2015 promoted similar strategies for increasing trustworthiness and security of digital services. (European Commission 2015). The *DSM Strategy* announced the review of the ePrivacy Directive 2002/58/EC in order to adapt it to the regulatory framework established by the General Data Protection Regulation (GDPR) 2016/679/EU that was passed by the European Parliament and the Council in 2016.

The GDPR attributes greater importance to the users' consent for data processing, implementing their fundamental right to privacy and the protection of their personal data. Despite the full harmonisation by the GDPR rules, questions remain, such as: How much information do consumers need in order to give well informed consent? For how long would the consent be valid? And perhaps even more complicated, is it acceptable to decline a service to customers who do not want to deliver personal data? With regard to tracking technologies the GDPR does not stipulate any specific rules, due to its concept of technology neutrality. However, the GDPR provides the background for the reassessment of the ePrivacy Directive 2002/58/EC.

In early 2017 the European Commission published a proposal to revise the ePrivacy Directive 2002/58/EC and to replace it by a directly binding regulation (European Commission 2017). The proposal lays down rules regarding the protection of fundamental rights and freedoms of natural and legal persons in the provision and use of electronic communications services – in particular, the rights to respect for private life and communications and the protection of natural persons with regard to the processing of personal data (Article 1). The material scope of the Regulation covers the processing of electronic communications data, which includes electronic communications content as well as electronic communications metadata (Article 4-3 (b) and (c)). The Regulation also provides protection for information stored in and related to end-users' terminal equipment (Article 8). In Recital 20, the draft regulation explicitly states that the end-users' terminal equipment connected to electronic communications networks and any information relating to the usage of such terminal equipment are part of the private sphere, protected by fundamental rights. It clarifies that such equipment contains or processes information that may reveal details of the location of individuals by accessing the device's geo-location capabilities. The information is related to such equipment and therefore requires enhanced privacy protection. Thus, any interference with the end-user's terminal equipment should be allowed only with the end-users' consent and for specific and transparent purposes. The legal requirements for the end-users' consent are defined in Articles 4 (11) and 7 of the

GDPR: Under that Regulation the data subject's consent must be freely given, specific, informed and unambiguous. The consent may be given by a written statement, including by electronic means, or an oral statement (GDPR, Recital 32). According to Recital 42 of the GDPR in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the extent to which consent is given. For consent to be informed, the data subject should at least be aware of the identity of the data controller and the purposes of the processing for which the personal data is intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice, or is unable to refuse or withdraw consent without detriment. In addition to that, Recital 43 of the GDPR states that consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all circumstances of that specific situation.

In the perspective of fundamental rights, prohibiting the most intrusive forms of data collection in order protect private life should also addressed. This can be relevant for some of the applications that have been made possible by geo-location. However, neither existing EU law nor the draft ePrivacy Regulation follow this strategy.

5.3 The EU's regulatory abstention for the use of geo-location data by security agencies

Regulating the use of tracking data by public authorities is also confronted by numerous legal questions yet to be answered (cf. Faßnacht 2012). Generally, security agencies tend to prefer working in a framework that is rather under- than overregulated (cf. Aden 2013 and 2016). A lack of specific democratic legislation leaves them more discretion for their work. Therefore, the use of tracking technologies for public security purposes is still under-regulated in most countries and in the EU.

While the draft ePrivacy Regulation includes legal requirements for the use of tracking technologies by private actors, the collection and processing of geo-location data for law enforcement purposes is not regulated at EU level. The draft ePrivacy Regulation does not apply to activities of competent authorities in the field of public security (European Commission 2017, Article 2-2 (d)). According to Article 87 (2) TFEU, the EU retains the authority to regulate the processing of tracking data in the framework of transnational police cooperation. In parallel with the GDPR, the European Parliament and the Council adopted

Directive (EU) 2016/680 *of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*. However, this directive does not include any rules for the use of tracking technologies. As the EU and its member states share legislation for issues related to the Area of Freedom, Security and Justice (AFSJ) (Article 4-2j TFEU), the member states can pass their own legislation on the use of geo-location tracking data for policing and security issues, so long as the EU does not adopt any rules for these specific purposes.

The rare court cases on GPS tracking by security agencies have not led to a more detailed approach so far. In *Uzun v. Germany*, the European Court of Human Rights found no violation of the right to private and family life (Article 8 of the European Convention of Human Rights), because the applicant was suspected to have been involved in serious crimes.[4] In times in which major threats are in the focus of the public debate, for example terrorist attacks, restrictive regulation of the security agencies' authority tends to be difficult to reach. More punitive measures will be easier to impose in such situations (cf. Garland 2001; Aden 2013). Nevertheless, a more concrete regulation would be helpful to define the purposes and types of cases for which security agencies may use geo-location to collect personal information. From the security agencies' perspective, clearer regulation would allow them to act with more legal certainty and legitimacy (cf. Aden 2013).

With regard to the fast development of new tracking technologies and their potential use for surveillance, at the very least, an adoption of minimum rules should be an issue for the EU.

6. Accountability for the use of tracking technology? Conclusion and outlook

As shown, geo-location has opened numerous new opportunities for useful applications facilitating everyday life, but also risks for far-reaching encroachments upon fundamental rights. Both security agencies and private actors should therefore be held accountable (in the sense of Bovens et al. 2014; Olsen 2014) for their use of tracking technologies. With regard to the transnational character of the technology and data processing, European and international regulation is necessary as current international law covering data processing is very

[4] ECtHR, Application no. 35623/05, judgment of 2 September 2010.

fragmented and far from the standard established in other fields as, for example, human rights or environmental protection.

An important question for regulation is related to the targets of surveillance. In political debates on surveillance it is mostly uncontested that individuals seriously threatening the security of others should be put under surveillance by security agencies within a rule of law system. However, a number of far reaching surveillance strategies that have been introduced during the last years, or that are currently under discussion, go far beyond this targeted surveillance. The retention of telecommunications metadata, for example, concerns all kinds of communications (telephone, internet, etc.) of all citizens without cause. Furthermore, the development of new technical tools allowing more precise and detailed surveillance must be taken into consideration with regard to the principles of proportionality. In sum, legal rules are needed to limit the use of this collected data to the purposes of targeted tracking and surveillance.

The question of accountability for the use of tracking technology remains one of the core elements of this debate. How much discretion should private actors and public security agencies have when they use geo-location? Which kinds of applications should be allowed, which prohibited? And which procedural safeguards are necessary to adequately protect the individuals' human rights?

References

Aden, Hartmut (2013) Polizei und das Recht: Stressquelle oder Stressvermeidung?, in: Rainer Prätorius& Lena Lehmann (eds.), Polizei unter Stress?, Frankfurt/Main: Verlag für Polizeiwissenschaft, 15-34.

Aden, Hartmut (2016) The Role of Trust for the Exchange of Police Information in the European Multi-level System, in: Jacqueline Ross & Thierry Delpeuch (eds.), Comparing the Democratic Governance of Police Intelligence. New Models of Participation and Expertise in the United States and Europe, Cheltenham, UK: Edward Elgar Publishing, 322-34

Bovens, Mark, Schillemans, Thomas &Goodin, Robert E.(2014)'Public Accountability', in: Mark Bovens, Thomas Schillemans& Robert E Goodin (eds.), The Oxford Handbook of Public Accountability, Oxford: Oxford University Press, 1-20.

Cohen, Elliot D. (2014) Technology of Oppression. Preserving Freedom and Dignity in an Age of Mass, Warrantless Surveillance, Basingstoke: Palgrave Macmillan.

European Commission (2010) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Agenda for Europe, COM(2010) 245 final.

European Commission (2015) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions, A Digital Single Market Strategy for Europe, COM(2015) 192 final.

European Commission (2017) Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and protection of personal data in electronic communications and repealing Directive 2002/58/EG (Regulation on Privacy and Electronic Communications), COM(2017) 10 final.

Faßnacht, Ute (2012) Rechtsfragen bei der Verwendung von Ortungstechnologien und einsatzunterstützender Systeme durch Feuerwehr und THW: rechtlicher Rahmen und Haftungsfragen, Münster: LIT Verlag

Garland, David (2001) 'The Culture of Control. Crime and Social Order in Contemporary Society', Oxford & New York: Oxford University Press.

Keller, Christian Michael (2008) Die Ermittlung der Kennungen und des Standorts von Mobilfunkgeräten im Spannungsfeld zwischen Kriminalitätsbekämpfung und Verfassungsmäßigkeit. Der Einsatz von IMSI-Catchern, Hamburg: Dr. Kovac.

Landau, Susan (2010) Surveillance or Security? The Risks Posed by New Wiretapping Technologies, Cambridge, MA: MIT Press.

Lyon, David (2015) Surveillance after Snowden, Cambridge: Polity Press.

Newman, Abraham L. (2012) The Governance of Privacy, in: David Levi-Faur (ed.), The Oxford Handbook of Governance. Oxford: Oxford University Press, 599-610.

Olsen, Johan P.(2014)'Accountability and ambiguity', in: Mark Bovens, Thomas Schillemans& Robert E Goodin (eds.), The Oxford Handbook of Public Accountability, Oxford: Oxford University Press, 106-123.