Location Privacy:
The Challenges of Mobile Service Devices

Introduction

The pervasive use of geo-location technologies poses new challenges to personal data and privacy protection, as they enable third parties to locate and track people and objects anywhere and at any time.[1] Although geo-location technologies have been part of our daily lives for a while, they have been confined largely to short-distance tracking and situations in which the user is fully aware that such technologies are being used, such as in the collection of tolls, the use of swipe cards on public transport, entry and exit cards to gain access to buildings and the use of Radio Frequency Identification (RFID) tags in library books or merchandise in shops.[2] However, the combination of ever-advancing technologies in geographical positioning systems (GPS), wireless-fidelity (Wi-Fi) and cellular identification has produced much more powerful location-based services (LBS) that can cover large distances. Furthermore, these technologies are often embedded in our mobile devices, which are connected invisibly and remotely to networks. Michael and Michael point out that such overarching location tracking and monitoring across all time and space has pushed us to live in a state of 'uberveillance', in which surveillance has become constant and embedded, and individuals and objects can be automatically located and identified.[3]

---

[1] Anne Uteck, 'Ubiquitous Computing and Spatial Privacy' in Ian Kerr, Valerie Steeves and Carole Lucock (eds), *Lessons from the Identity Trail* (OUP, 2009) 83.

[2] Karl D. Stephan, Katina Michael, M.G. Michael, Laura Jacob and Emily P. Anesta, 'Social Implications of Technology: The Past, the Present, and the Future' (2012) 100 Proceedings of the IEEE 1752. For a discussion of RFID, see Marcus R. Wigan & Roger Clarke, 'Big Data's Big Unintended Consequences' (2013) 46:6 IEEE Computer 46–53.

[3] M.G. Michael and Katina Michael, 'Toward a State of Überveillance' (2010) 29(2) IEEE Technology and Society Magazine, 9.

In other words, while we as consumers are using these technologies much more extensively, they are in turn using us as consumers. Not only do devices such as smartphones, laptops, iPads and computer tablets disclose where we are and when and what we are doing, they also enable telecommunications companies or Internet service providers to record our activities. In revealing the unique combination of the location, time and content of our activities, they allow data about us to be sent to others for analysis and for subsequent profiling.[4] The smart mobile devices that we carry with us have in fact become tools for surveillance, yet many of us have embraced them willingly, albeit unwittingly. The potential for abuse of personal data and the threats to privacy that arise from government and commercial entities using geo-location technologies are enormous. Dobson and Fisher warn about the hazards of 'geoslavery', whereby a person's physical location is coercively or surreptitiously monitored or controlled by another.[5] Litigation and academic debate have already emerged concerning the possible violation of the constitutional right to privacy that might arise from the government's use of geo-location technologies for law enforcement without a judicial warrant.[6] In 2012, the US Supreme Court condemned the use of GPS

[4] For larger implications, Katina Michael and M. G. Michael, 'The Social and Behavioural Implications of Location-Based Services' (2011) 5:3-4 Journal of Location Based Services 121.

[5] Jerome E. Dobson and Peter F. Fisher, 'Geoslavery' (2003) (Spring Issue) IEEE Technology and Society Magazine 47. William A. Herbert. 'No Direction Home: Will the Law Keep Pace With Human Tracking Technology to Protect Individual Privacy and Stop Geoslavery' (2006) 2:2 Journal of Law and Policy for the Information Society 409.

[6] This is discussed under protection against search and seizure of the Fourth Amendment of the US Constitution and Section 8 of the Canadian Charter of Rights and Freedom. David H. Goetz, 'Locating Location Privacy' (2011) 26 Berkeley Tech. L.J. 823. Teresa Scassa, 'Information Privacy in Public Space: Location Data, Data Protection and the Reasonable Expectation of Privacy' (2009) 9:2 Canadian Journal of Law and Technology 193. For an overview of legal inadequacies in the US, the European Union and Australia, see Katina Michael and Roger Clarke, 'Location and Tracking of

technologies to track the movements of suspects without a warrant, and deemed the practice to be in violation of the Fourth Amendment of the Constitution.[7] Another strand of the literature covers the gross breaches of personal data privacy and autonomy that arise when consumer profiling is carried out on the pretext of better service planning and more efficient advertising and marketing.[8]

Adding to the current debate, this article focuses on the personal data and privacy challenges posed by private industry's use of smart mobile devices that provide location-based services to users and consumers. Directly relevant to personal data protection are valid concerns about the collection, retention, use and accessibility of this kind of personal data, in relation to which a key issue is whether valid consent is ever obtained from users. While it is indisputable that geo-location technologies serve important functions, especially in cases of emergency and rescue,[9] their potential use for surveillance and invasion of privacy should not be overlooked. Thus, in this study we address the question of how a legal regime can ensure the proper functionality of geo-location technologies while preventing their misuse. In doing so, we examine whether information gathered from geo-location technologies is a

---

'Mobile Devices: Überveillance Stalks the Streets' (2013) 2 Computer Law & Security Review 29.

[7] US v. Jones, 565 U.S. (2012). Peter Swire, 'A Reasonableness Approach to Searches after the *Jones* GPS Tracking Case' (2012) 64 Stanford Law Review Online 57. For a general discussion, see James M. Thurmana, 'US Courts Confront GPS Surveillance: Is *Maynard* a Harbinger of Change or an Anomaly? (2011) 5 Journal of Location Based Services 201.

[8] Roger Clarke and Marcus Wigan, 'You Are Where You've Been: The Privacy Implications of Location and Tracking Technologies' (2011) 5 Journal of Location Based Services 135.

[9] Anas Aloudat, Katina Michael, Xi Chen, and Mutaz Al-Debei. 'Social Acceptance of Location-Based Mobile Government Services for Emergency Management' (2013) 30 Telematics and Informatics <http://www.sciencedirect.com/science/article/pii/S0736585313000051> accessed 30 August 2013.

form of personal data, how it is related to privacy and whether current legal protection mechanisms are adequate. We argue that geo-location data are indeed a type of personal data. Not only is this kind of data related to an identified or identifiable person, it can reveal also core biographical personal data. What is needed is the strengthening of the existing law that protects personal data (including location data), and a flexible legal response that can incorporate the ever-evolving and unknown advances in technology.

To examine the above issues, Part I of this article defines the meaning of location data, and highlights the problems concerning the surreptitious acquisition of location data and the equally problematic issue of uninformed consent in the seemingly voluntary disclosure of location data in consumers' increasing adoption of geo-location technologies. Part II identifies the legal implications in the personal data protection regimes in the European Union (EU) and the US. EU law is an obvious choice in studying this topic, as it is impossible to ignore the EU's comprehensive and elaborate legal scheme of personal data protection, especially its extraterritorial effect in requiring an adequate level of protection in countries where the data are received.[10] In contrast, the choice to study the US approach may be puzzling to some, as personal data protection has been described as 'fragmented' and often depends on the type of

[10] Article 25 of the Data Protection Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. Official Journal L 281, 23/11/1995 P. 0031 – 0050 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML> accessed 10 September 2013. Rolf H. Weber, *Regulatory Models for the Online World* (Kluwer Law International, 2002) 156.

data and the entities in control.[11] Nevertheless, Solove and Hartzog argue that the US position is worth studying because of an emerging jurisprudence based on the large number of settlement cases and decisions from the Federal Trade Commission, which has played a pivotal role in influencing the development of personal data regulations, policies and company practices.[12] Due to the globalised nature of technology companies, it is necessary to understand the US legal landscape. After identifying the loopholes in the present legal regimes regarding the protection of location data, the legal reforms proposed by the EU and the US are examined to address this issue.[13] In reviewing the challenges posed by geo-location technologies and analysing the issues in the current legal debate, we aim to find ways to strengthen the existing laws to ensure they protect location data. In this article, the terms 'location data' and 'location information' are used interchangeably, mainly because location data is a legal term used in the EU, whereas location information is used in the US.[14]

---

[11] Daniel J. Solove and Woodrow Hartzog, The FTC and the New Common Law of Privacy, 15 August 2013 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2312913> accessed 8 September 2013.

[12] Although the study by Solove and Hartzog focuses on the decisions of the Federal Trade Commission, companies have been looking into settlement agreements and law to guide their privacy practices and policies.

[13] For the European position, see the European Commission's 'Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals 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 the free movement of such data,' 25 January 2012, <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_10_en.pdf> accessed 17 April 2013. For the US position, see the Location Privacy Act of 2011, S. 1223, 112th Congress (2011-2012) <http://www.govtrack.us/congress/bill.xpd?bill=s112-1223> accessed 17 April 2013.

[14] For a discussion on the nuances between 'personally identifiable information' and 'personal data', see William B. Baker and Anthony Matyjaszewski, 'The Changing Meaning of "Personal Data"'(*International Association of Privacy Professionals Resource Center*, 30 September 2010) <https://www.privacyassociation.org/resource_center/the_changing_meaning_of_personal_data> accessed 21 April 2013.

I. Geo-location Information, Technologies and Privacy

A. Location and Geo-Location Information

The rapid development and enhancement of modern positioning technologies has facilitated the collection of location information, making it possible for us to examine various aspects of other people's lives. By the term 'location information', we mean any type of data that places an individual at a particular location at any given point in time, or at a series of locations over time.[15] It also encompasses geo-positioning other than latitude, longitude and altitude, which can be ascertained with varying degrees of precision.[16] A data picture of an identifiable individual can be created with the combination of the above location information.[17] The elements of space, time and content are the core of location information[18] although the descriptive aspect, or the type of location, is the most important and revealing.[19] For instance, by detecting that an individual visits a mosque every week, we may be able to infer his or her likely religious affiliation.[20] Roger Clarke describes this as tracking the

---

[15] Scassa (n. 6) 193.

[16] Roger Clarke, 'Person-Location and Person Tracking: Technologies, Risks and Policy Implications' (2001) 14:2 Information Technology & People, 206 at 208.

[17] Scassa (n. 2) 193.

[18] George Cho, 'Geographic Information Science, Personal Privacy, and the Law' in John P. Wilson and A. Stewart Fotheringham (eds), *The Handbook of Geographic Information Science* (Blackwell, 2008) 526-527.

[19] Bennett and Crowe explain that location information has three dimension of being geo-spatial, civic and descriptive. While geo-spatial refers to the positioning on the globe through longitude, latitude and altitude, and civic refers to the locational coordinates that are provided as a result of political decisions concerning borders, it is the descriptive aspect that reveals the immediate type of location that one is in or has visited at a certain time. Colin J. Bennett and Lori Crowe, 'Location-Based Services and the Surveillance of Mobility: An Analysis of Privacy Risks in Canada' A Report to the Office of the Privacy Commissioner of Canada (June 2005) 33 <http://www.colinbennett.ca/wp-content/uploads/2012/06/OPCREPORTFINAL.pdf> accessed 17 April 2013.

[20] Mark N. Gasson, Eleni Kosta, Denis Royer, Martin Meints, and Kevin Warwick, 'Normality Mining: Privacy Implications of Behavioral Profiles Drawn from GPS Enabled Mobile Phones' (2011) 41:2 IEEE Transactions on Systems, Man and Cybernetics, 251 at 258

'virtual space' of an individual, revealing his or her successive interactions with a particular organisation.[21] Clarke also defines tracking as 'the plotting of the trail, or sequence of locations, within a space that is followed by an entity over a period of time.[22] The specific term 'geo-location information' refers to the information generated by electronic devices that can be used to determine the location of the relevant devices and their users.[23] This has been made possible by the introduction of location-based services (LBS) in wireless mobile devices, which allow real-time tracking to be used widely and easily by consumers.[24] With LBS, location data have gained additional and richer dimensions by readily revealing a person's direction of travel and trajectory, or even his or her predicted movements.[25] From the above perspective, location information necessarily includes geo-location information.

At this point, we may question whether knowing a person's location or movement in public places should be subject to privacy protection, as the individual concerned is already in the public arena.[26] To understand the relationship between location data, personal data and privacy, and the implications of allowing commercial entities to use location data, we need to

---

<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5599314> accessed 26 August 2013.

[21] Clarke (n. 16).

[22] ibid.

[23] Definition of geo-location information from s. 2601 of the proposed *Geolocational Privacy and Surveillance Act* in the United States, H.R. 1312, 113th Congress, introduced in March 2013 <http://beta.congress.gov/bill/113th/house-bill/1312> accessed 31 August 2013.

[24] Bennett and Crowe (n. 19) 32.

[25] Sjaak Nouwt characterises the latter two categories as traffic data and movement data. Sjaak Nouwt, 'Reasonable Expectations of Geo-Privacy' (2008) 5(2) Scripted 375, 376. For the relations on personal data and profiling, see Mireille Hildebrandt, 'The Dawn of a Critical Transparency Right for the Profiling Era' in Jacques Bus, Malcolm Crompton, Mireille Hildebrandt and George Metakides (eds), *Digital Enlightenment Yearbook* (Amsterdam: IOS Press, 2012). <http://works.bepress.com/mireille_hildebrandt/40> accessed 26 August 2013.

[26] Helen Nissenbaum, *Privacy in Context* (Stanford University Press, 2010) 103-128.

understand how geo-location technologies work and the nature of the location data that are being revealed.

B. Geo-Location Technologies

For LBS to work and to determine users' location requires the involvement of geographical positioning system (GPS), cellular identification, Wi-Fi and Assisted-GPS (A-GPS) technologies.[27]

GPS is dependent on a constellation of 24 satellites to give accurate positional information on the four dimensions of latitude, longitude, altitude and time.[28] It works best outdoors, providing positioning accuracy between 4 and 15 meters.[29] However, it is battery intensive and inconsistent or unavailable indoors.

Cellular identification uses the technique of triangulation.[30] When a mobile device is switched on, it is linked to a specific base station with a unique ID registered to a specific location. A mobile device can be located based on the estimation of the direction from which

[27] Another common positioning technology, but not the subject matter of discussion of this article, is radio-frequency identification which 'utilizes tags with computer chips containing digital information that can used to track and identify humans, animals and inanimate objects.' Herbert (n. 5), 412 n. 7. It is commonly used in tracking products from manufacturers to consumers. Wigan and Clarke (n. 2).

[28] A. Roxin, J. Gaber, M. Wack and A. Nadit-Sidi-Moh, ,'Survey of Wireless Geolocation Techniques' in *Proceedings of IEEE-GLOBECOM'07, Workshop SUPE'07,* 26-30 November 2007, Washington , DC, USA. <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4437809> accessed 18 September 2013.

[29] Janice Y. Tsai, Patrick Gage Kelley, Lorrie Faith Cranor, Norman Sadeh, 'Location-Sharing Technologies: Privacy Risks and Controls' (2010) <http://cups.cs.cmu.edu/LBSprivacy/files/TsaiKelleyCranorSadeh_2009.pdf> accessed 17 April 2013.

[31] Roxin, Wack and Nadi-Sidi-Moh (n. 28).

its signal arrives at the base station.[31] This method provides a quick indication of location, but is only accurate to approximately 50 meters in densely populated urban areas and up to several kilometres in rural areas.[32]

In contrast, Wi-Fi can locate devices in areas that have become blanketed with both personal and public Wi-Fi access points.[33] It relies on a unique ID from the WiFi access point, which can be detected by a mobile device and sent to a service that provides a location for each unique ID. The unique ID for each Wi-Fi access point is its MAC address (Medium Access Control), which is recorded in the hardware of the device . Like radio, the Wi-Fi enabled devices continuously transmits its own network name and its MAC address so that it can be located. While it may not provide as precise a location as GPS, this technology is more widely used and can function well indoors.

Another geo-location technology is assisted GPS (A-GPS), a hybrid solution that can speed up the location process. Information about the mobile device is transmitted through the network of base stations to speed up the location process, which only takes a few seconds.[34] This combination of GPS and cellular identification technology can resolve the long delays that can occur when locating by GPS alone due to obstructions that block the view from the

[31] Roxin, Wack and Nadi-Sidi-Moh (n. 28).
[32] ibid.
[33] ARTICLE 29 Data Protection Working Party, 'Opinion 13/2011 on Geolocation Services on Smart Mobile Devices' adopted on 16 May 2011 <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf> accessed 17 April 2013.
[34] Roxin, Gaber, Wack and Nait-sidi-Moh, (n. 28).

handset to the GPS satellite.[35] However, as the following discussion highlights, many people may have embraced these new smart mobile gadgets and new LBS without fully realising their invasive potential.

C. Surreptitious Acquisition of Geo-Location Data

1. Mapping of Wi-Fi Router Location and Harvesting Wi-Fi Data

Many people have used Google maps to find local businesses and restaurants, get driving or walking directions or simply to view maps. Few of them, however, would have realised that the location of their mobile devices, through Wi-Fi connections, were also being mapped and could easily be found by others on the Internet.[36] In 2011, McCullagh reported that Google had published the estimated locations of millions of iPhones, laptops and other devices with Wi-Fi connections.[37] This was possible because Wi-Fi enabled devices (including personal computers, iPhones, iPads and Android phones) with location-based services enable regular beaming of their unique hardware identifiers, or MAC addresses (the ID number of the Wi-Fi network's hardware), back to their base stations. Making this information available means that it is possible to find the physical address associated with a person from their MAC address. Bearing in mind that by June 2011 there were already one

[35] ibid.
[36] Declan McCullagh, 'Exclusive: Google's Web Mapping can Track Your Phone' (*CNET*, 15 June 2011) <http://news.cnet.com/8301-31921_3-20070742-281/exclusive-googles-web-mapping-can-track-your-phone/> accessed 17 April 2013.
[37] ibid.

billion Wi-Fi enabled mobile phones,[38] the implications for location information collection are not hard to foresee.

Furthermore, according to McCullagh, Google had been harvesting WiFi data and the MAC addresses and network SSIDs (the user-assigned network ID name) tied to the location data of private wireless networks.[39] Google also admitted that it had intercepted and stored Wi-Fi transmission data, including email passwords and email content, from their Google Street View cars.[40] By January 2011, the regulatory authorities in at least 12 countries were investigating Google over this matter,[41] and Google's practice has been condemned in various jurisdictions.[42] The France Data Protection authority (CNIL) denounced Google Street View's practice of scooping up personal data from Wi-Fi networks and imposed a fine of 100,000 euros on the company.[43] Google itself admitted collecting 600 gigabytes of data from more than 30 countries.[44]

---

[38] Norman Sadeh, 'Mobile Location Privacy: Forces at Play, Attitudes and Challenges' (Mobile Commerce Lab, Carnegie Mellon University, 2 June 2011) <http://www.ecom-icom.hku.hk/seminar/20110602/Sadeh.pdf> accessed 17 April 2013.

[39] ibid.

[40] See Google's public acknowledgement: 'Data collected by Google cars' (Google Europe Blog, 27 April 2010) <http://googlepolicyeurope.blogspot.hk/2010/04/data-collected-by-google-cars.html>; ' WiFi data collection: An update' (Google Official Blog, 14 May 2010) <http://googleblog.blogspot.hk/2010/05/wifi-data-collection-update.html> accessed 15 May 2013.

[41] EPIC, 'Investigations of Google Street View', < http://epic.org/privacy/streetview/ > accessed 17 April 2013.

[42] An overview of the responses of different countries can be seen from Electronic Privacy Information Center, 'Investigations of Google Street View' http://epic.org/privacy/streetview/ accessed 21 April 2013.

[43] Commission Nationale de l'Informatique et des Libertés, 'Google Street View: CNIL pronounces a fine of 100,000 Euros' (CNIL, 21 March 2011) <http://www.cnil.fr/english/news-and-events/news/article/google-street-view-cnil-pronounces-a-fine-of-100000-euros/> accessed 24 May 2013.

[44] 'WiFi data collection: An update' (Google Official Blog, 14 May 2010) <http://googleblog.blogspot.hk/2010/05/wifi-data-collection-update.html> accessed 15 May 2013 (see note 40 above).

In the United States, citizens from 10 different states brought a class action against Google Street View in 2011, contending that Google had violated the federal Wiretap Act and other related state legislations by intercepting their data packets, including MAC addresses, SSID information (Wi-Fi network name), usernames, passwords and personal emails through the Wi-Fi system *In re Google Inc. Street View Electronic Communications Litigation*.[45] Contrary to the belief that the collection of Wi-Fi data was an accident and a technical blunder, the court found that back in 2006, Google engineers had intentionally created a data collection system that could sample, collect, decode and analyse all types of data broadcast though Wi-Fi connections.[46] Moreover, it was found that Google had authorised the inclusion of the above system, known as wireless sniffer technology, into its Google Street View vehicles and patented the process.[47] While at the time of writing the full trial of the above case was still pending, in 2013 Google paid US$7 million in settlement of a class action brought by 38 states on a similar issue of unauthorised Wi-Fi data harvesting by Google Street View cars.[48]

---

[45] 794 F.Supp.2d 1067, N.D.Cal., 2011. The issue before court at that round was just on the preliminary point whether Google was allowed to rely on the exemption clause of s. 2510(16) of the Wiretap Act to dismiss the plaintiffs' motion based on the reason that the data collection was from open Wi-Fi networks which are 'readily accessible to the general public,' which the court ruled against Google on that point.

[46] ibid. See also Roya Nikkhah, 'Google Apologises for Collecting Personal Web Data' *The Telegraph* (UK, 15 May 2010) <http://www.telegraph.co.uk/technology/google/7727907/Google-apologises-for-collecting-personal-web-data.html> accessed 16 April 2013.

[47] Ibid.

[48] 'Attorney General Announces $7 Million Multistate Settlement with Google over Street View Collection of WiFi Data' (State of Connecticut, 12 March 2013) <http://www.ct.gov/ag/cwp/view.asp?Q=520518&A=2341> accessed on 21 May 2013.

2. Tracking through Smart Phone Operating Systems

Other than Google, Microsoft and Apple have also been found to have acquired location data surreptitiously from their customers. For instance, in 2011, a class action was filed against Microsoft before the Seattle Court in the US for tracking the location of its mobile customers using Windows Phone 7, in direct contravention of customers' requests not to be tracked.[49] At the same time, Apple iPhones were also reported to be tracking users, collecting their location data (including timestamps) and storing it for up to a year, even when the location software was turned off.[50] It was reported that the data were also saved in a secret file on a device on the iPhone, which was then copied to the owner's computer when the two were synchronised by Apple programmes.[51] It is not certain why Apple was storing the data

[49] Rebecca Cousineau and others v. Microsoft Corporation, Case 2:11-cv-01438-JCC Document 19 Filed 10/17/11 < http://static.withinwindows.com/files/uploads/2011/10/Doc19_101711.pdf> accessed 17 April 2013. In June 2012, Microsoft applied to dismiss the case, in which the Court granted the motion to dismiss under the Wiretap Act, Washington Consumer Protection Act, Washington Privacy Act, and unjust enrichment claims, but denied it with respect to the plaintiff's claim under the Stored Communications Act. Rebecca Cousineau and others v. Microsoft Corporation, Case 2:11-cv-01438-JCC Document 38 Filed 06/22/12 <http://newsandinsight.thomsonreuters.com/uploadedFiles/Reuters_Content/2012/06_-_June/gibson_microsoft.pdf > accessed 30 January 2013.

[50] Alasdair Allan and Pete Warden, data scientists and former Apple staff, discovered this hidden function in 2011. Charles Arthur, 'iPhone Keeps Record of Everywhere You Go' *The Guardian* (20 April 2011) <http://www.guardian.co.uk/technology/2011/apr/20/iphone-tracking-prompts-privacy-fears> accessed 17 April 2013.

[51] The file is known as consolidated.db. Alasdair Allan and Pete Waren, 'Got an iPhone or 3G iPad? Apple is recording your Moves' (*O'Reilly Radar*, 20 April 2011) < http://radar.oreilly.com/2011/04/apple-location-tracking.html> accessed 17 April 2013. Apple admitted on April 27 that the alleged track did happen. But it maintained that the track was done unintentionally and other faults were due to "bugs". See 'Apple Q&A on Location Data' (Apple Press Info, 27 April 2011) <http://www.apple.com/pr/library/2011/04/27Apple-Q-A-on-Location-Data.html> accessed 23 September 2013. Apple released an update of iOS in the following May. See Chloe Albanesius, 'Apple Releases iOS 4.3.3 With Location Fixes' (PCMag.com, 4 May 2011) <http://www.pcmag.com/article2/0,2817,2384903,00.asp> accessed 23 September 2013.

or how it intended to use it, but what is certain is that with a simple programme,[52] anyone (including the owner's partner, a private detective or a stranger) who had access to a person's iPhone or other Apple device could have discovered the details about the owner's movements. In 2011, Apple was fined 3 million Korean Won (US$2855) by the Korea Communications Commission for collecting the location information of users despite their withdrawal of consent.[53] Although the amount was negligible to a giant corporation, Michael and Michael point out that it sent an important warning message to Apple and other tech giants to be socially responsible.[54]

D. Voluntary Disclosure of Geo-Location Data: Full Consent?

Although often we may be unaware that our devices or our locations are being mapped for others to see, and that our data are being secretly collected by others, sometimes we voluntarily agree to be the targets of tracking or we may seek to track others. The use of tracking as part of location-based sharing in a social context can be a sign to show who one's 'buddies' are,[55] which is seen as essential for self-representation.[56]

---

[52] Alasdair Allan and Pete Waren, 'iPhone Tracker' <Petewarden.github.com/iPhoneTracker> accessed 17 April 2013.

[53] This was in violation of Article 15 of the Location Privacy Protection Act of South Korea. Korea Communications Commission, Press Release KCC requests Apple and Google to take corrective action with regard to their violation of the Location Privacy Protection Act and fines them, 3 August 2011 <http://eng.kcc.go.kr/user.do?mode=view&page=E04010000&dc=E04010000&boardId=1058&cp=7&boardSeq=32046> accessed 18 September 2013.

[54] Michael and Michael (n. 4) 129.

[55] Sarah Jean Fusco, Roba Abbas, Katina Michael and Anas Aloudat, 'Location-Based Social Networking: Impact on Trust in Relationships' (2012) 31:2 IEEE Technology and Society Magazine 39 <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6213869> accessed 26 August 2013.

[56] Vassilis Kostakos, Jayant Venkatanathan, Bernardo Reynolds, Norman Sadeh, Eran Toch, Siraj A.

Seemingly, users of social networking sites have given their express consent to share their location information with their 'buddies'. In practice, however, the scope of consent has often exceeded users' expectations. Although it is common practice for personal data to be collected and shared between data users and advertisers, most users are not aware that their data are being accessed and shared by unknown third parties.[57] The Electronic Privacy Information Center in the United States reported that Facebook Places had made users' location data routinely available to others, including Facebook business partners, so that Facebook could sell users' current locations and profiles to stores in their vicinity, which could then deliver hyper-targeted advertising to them.[58] By default, check-in information on Facebook is available not only to the third-party developers of applications that a user has authorised, but also to the third-party developers of applications that a user's friends have authorised.[59] Another worrying feature is that there is no single opt-out feature to avoid location tracking from Places.[60] Thus, concerns have been raised on whether there is full

---

Shaikh, Simon Jones 'Who's Your Best Friend? Targeted Privacy Attacks in Location-Sharing Social Networks' in proceedings of Ubicomp 2011, Beijing, China, pp. 177-186 (2011) < http://www.ee.oulu.fi/~vassilis/files/papers/ubicomp11.pdf> accessed 17 April 2013.

[57] Jennifer M. Urban, Chris Jay Hoofnagle, and Su Li, 'Mobile Phones and Privacy' 11 July 2012 <http://ssrn.com/abstract=2103405> accessed 8 September 2013. The study interviewed 1200 households in the United States, and 70% indicated that they would not allow cell phone providers to use their location data. This was on the basis that the consumers were aware of and given the choice.

[58] The Electronic Privacy Information Center, 'Facebook Places and Privacy' August 2010 <http://epic.org/privacy/facebook/places/> accessed 26 August 2013. See Facebook's own introduction to Places, 'Who, What, When, and Now...Where' (The Facebook Blog, 18 August 2010) <http://blog.facebook.com/blog.php?post=418175202130> accessed 21 May 2013.

[59] ibid.

[60] According to EPIC, users who do not want their location information revealed to others have to (1) disable 'Friends can check me in to Places' (2) customise 'Places I Check In', (3) disable 'People Here Now,' and (4) uncheck 'Places I've Visited'. *Ibid*. Denoja Kankesan, 'How to Check Out of Facebook's New Personal Locator' CBC News, 24 August 2010 <http://www.cbc.ca/news/technology/story/2010/08/24/f-facebook-places-privacy.html>.

disclosure of information and whether valid consent is ever obtained.

Computer scientists have also warned about the problem of geo-tagging: the process of adding location information to documents that are uploaded online by the users themselves.[61] Freidland and Sommer pointed out that this technology is commonly used, but not all users are aware of it.[62] For instance, all iPhones include in-built high-precision geo-coordinates with all photos and videos taken with the internal cameras. Other major smartphone makers also offer models allowing instantaneous uploading of geo-tagged photos, videos and text messages onto Flickr, YouTube and Twitter. Other than the fact that users may not know that their location information is being shared when they upload their items online, the location data that they have uploaded can be used to cross-reference information from other publicly available online content, so that the exact addresses of potential victims can be identified to mount real-world privacy attacks. Friedland and Sommer were able to use geo-tagged photos randomly selected from an online advertisement site, together with information from Google Street View, to find out the exact postal addresses of sellers.[63] In addition, with the geo-tagging information from photos and Twitter feeds, they were able to find out the address of and the places frequented by one particular celebrity.[64] This means that even if an individual has made a conscious choice not to share his location information, he may still be

[61] Gerald Friedland and Robin Sommer, 'Cybercasing the Joint: On the Privacy Implications of Geo-Taggin' Paper for Proc. USENIX Workshop on Hot Topics in Security, 2010 <http://www.icsi.berkeley.edu/pubs/networking/cybercasinghotsec10.pdf > accessed 16 September 2013.
[62] ibid.
[63] ibid.
[64] ibid.

tagged if his photo is taken by a third party using geo-tagging technology.

Another concern associated with the use of mobile devices is the rapid explosion of 'apps' and their potential to invade privacy. Apps are games and software applications for smartphones and other wireless mobile devices. In 2010, the *Wall Street Journal* studied 101 popular smartphone apps and revealed that 56 of them transmitted the phone's unique device ID to other companies, 47 transmitted the phone's location and five sent users' age, gender and other personal details to outsiders without their consent or awareness.[65] Although Apple Inc. (which makes the iPhone) and Google Inc. (which developed the Android operating system) claimed that they protected users by requiring all apps to obtain permission before revealing certain kinds of information, including location-based data, the *Wall Street Journal* study revealed the contrary. The study showed that 45 apps did not provide privacy policies for consumers to select. Furthermore, it was found that many iPhone apps had sent users' locations to advertising networks without informing users.[66] Equally worrying, a study of 50 Android apps conducted by *The Sunday Times* in 2012 found that six companies gave the apps' creators the right to read SMS messages stored on the users' devices or Sim cards.[67] These companies included Facebook, Yahoo!, Flickr and Badoo. Another app tracked the

[65] An example of the last category of apps the popular social networking site MySpace, which sent the age, gender, income, ethnicity, parental status and device ID of its users to Millennial Media, a giant advertisement network company. Scott Thurm and Yurai Iwatani Kane, 'Your Apps are Watching You' *The Wall Street Journal* (17 December 2010) <http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html> accessed 17 April 2013.

[66] ibid.

[67] Robin Henry and Cal Flyn, 'Smartphone Apps that Cash in on your Privacy' *The Sunday Times* (26 February 2012) 10.

user's location by means of GPS, see the entire web browser's history and identify the user's email address and profile.[68] If app users knew how much information was being accessed by third parties, it is unlikely that they would give their consent.[69]

The above figures from the media are alarming because they expose the various aspects of privacy invasion through apps and smartphones. First, we now know that location tracking by marketing companies is pervasive and invasive. In 2009, even before location-based advertising became common practice, online behavioural advertising and targeting had drawn the attention of the US Federal Trade Commission. This problem had already prompted the Commission to come up with specific guideline for consumer data protection.[70] Now, with apps and their location-based tracking and powerful personalised targeting, challenges to privacy and security have become more acute and intense. Advertising companies claim that user data are aggregated and not linked to individuals, and they are only interested in targeting phone users by location, type of device and demographic data, yet these companies have in fact gathered personal data that could be linked to identifiable individuals.[71] As the *Wall*

[68] The app is called Justin Bieber Droid Wallpapers, *ibid*.
[69] According to a 2012 nationwide survey of 2254 adults by the Pew Research Centre in the US, 54% of app users decided not to install a cell phone app after they discovered how much personal data they would need to share to use it. Jan Lauren Boyles, Aaron Smith and Mary Madden, 'Privacy and Data Management on Mobile Devices' Pew Internet Reports, 5 September 2012, <http://pewinternet.org/Reports/2012/Mobile-Privacy.aspx> accessed 27 January 2013.
[70] US Federal Trade Commission Staff Report: Self-Regulatory Principles for Online Behavioral Advertising (February 2009) <http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf> accessed 17 April 2013. For further discussion, Dorothy M. Bollinger and Tristram R. Fall III, 'Current Developments in Privacy and Security – Impact of Technology' 82 Pennsylvania Bar Association Quarterly 139 (2011).
[71] The companies interviewed by the *Wall Street Journal* include Traffic Marketplace, and Mobclix. The latter had 25 ad networks with 15,000 apps seeking advertisers. See Thurm and Kane, 'Your Apps are Watching You' (n 65).

Street Journal study showed, the most commonly collected data are the unique device identifiers on smart phones set by the phone makers, carriers or makers of the operating systems, which cannot be blocked or deleted. Second, in many cases, as revealed in the report, smartphone users are not given an 'opt in' option for phone tracking, which means users' express consent is never sought. Third, different app companies have different interpretations on what qualifies as personal data, and a study for the *Future of Privacy Forum* in 2011 found that 22 of the 30 most popular mobile apps in the US did not have any privacy policy.[72] This problem should not be underestimated, especially in light of the fact that by May 2009, Skyhook Wireless, which provides WiFi positioning for Apple Products and AOL, was already receiving 250 million location requests every day.[73] It is further estimated that by 2016, the worldwide mobile app industry will achieve 44 billion downloads.[74]

E. Wider Implications

Locating or tracking a person's whereabouts can be potentially invasive and dangerous, which raises valid concerns over whether information concerning one's location may be misused by others. Scholars have also pointed out the potential for abuse in using GPS

[72] Future of Privacy Forum, 'FPF Finds Nearly Three-Quarters of Most Downloaded Mobile Apps Lack a Privacy Policy' 12 May 2011 <http://www.futureofprivacy.org/2011/05/12/fpf-finds-nearly-three-quarters-of-most-downloaded-mobile-apps-lack-a-privacy-policy/> accessed 17 April 2013.

[73] Centre for Democracy and Technology, 'Location Information is Poorly Protected in the Commercial Context' 2 March 2010 <http://cdt.org/policy/cdt-testifies-location-privacy> accessed 17 April 2013.

[74] Future of Privacy Forum, 'Future of Privacy Forum Launches App Privacy Site' 16 May 2011 <http://www.futureofprivacy.org/2011/05/26/future-of-privacy-forum-launches-app-privacy-site/> accessed 17 April 2013.

technologies in social relationships such as parenting, employment, insurance, intimate partnerships and online social sharing.[75]

In relatively mild cases, the tracking function will facilitate 'helicopter parents' to check up on their children.[76] Employers may also request tracking of their employees. As a research experiment, Professor Norman Sadeh of Carnegie Mellon University introduced a programme to track his research assistants, to see where they were when they were late.[77] Accounts of employers using LBS to track their workers (mostly mobile workers such as truck drivers, postal workers and couriers) with mobile phones, and of car rental companies and insurance companies raising their fees after discovering through mobile devices that their customers had violated contractual terms, are well documented.[78]

Social tracking may have wider security implications. The general fear is for people's physical safety, such as stalking by third parties. A special report by the US Department of Justice in 2009 revealed that there were about 26,000 victims of GPS stalking in 2006, representing nearly 10% of stalking victims in that year.[79] The use of GPS technologies by

---

[75] Roba Abbas, Katina Michael, M.G. Michael, and Anas Aloudat, 'Emerging Forms of Covert Surveillance Using GPS-Enables Devices' (2011).

[76] The term is used to describe over-involved parents who like to know where their children are and need to check up their children all the time. Jeffrey R. Young, 'Now You can Track Colleagues and Students on Your Laptop' 55 (25) *The Chronicle of Higher Education*, 27 February 2009, A15.

[77] Young, ibid.

[78] Bennett and Crowe (n. 19). Katina Michael and Gregory Rose, 'Human Trafficking Technology in Mutual Leal Assistance and Police Inter-state Cooperation in International Crimes' in *From Dataveillance to Uberveillance and the Realpolitik of the Transparent Society* (University of Wollongong, 2007) 241 <http://ro.uow.edu.au/cgi/viewcontent.cgi?article=1559&context=infopapers> accessed 3 September 2013.

[79] Katrina Baum, Shannon Catalano, Michael Rand and Kristina Rose 'Stalking victimization in the United States' (Washington, DC: US Department of Justice 2009) 5 <http://www.ovw.usdoj.gov/docs/stalking-victimization.pdf> accessed 1 September 2013.

former partners to kidnap or track their former spouses has caused serious problems.[80] One problem with over-sharing and the 'malicious potential of systematic location-based search' [81]is the danger of inviting break-ins to one's property, as illustrated humorously and vividly by the site 'Pleaserobme.com,' [82] where a stream of updates from various location-based networks (including Foursquare and Twitter) show when users check-in somewhere, indicating that they are not in their homes.

As we have seen, the flourishing of geo-location-based technologies has brought new challenges to the ecosystem of mobile applications, consumer culture and social media. The nature and scope of the information that such technology reveals about individuals is troubling, and raises legitimate concerns over privacy and personal data violations.

II. A Study of Legal Regulations: The EU and the US Models

Some may argue that when individuals are in a public place, they can hardly claim the

[80] Justin Schenk, 'Stalkers Exploit Cellphone GPS' Wall Street Journal, 3 August 2010 <http://blogs.law.nyu.edu/privacyresearchgroup/wp-content/uploads/Stalkers-Exploit-Cellphone-GPS-Mobile-Location-Tracking-WSJ.com_.pdf> accessed 3 September 2013. In Villanova v. Innovative Investigations, Inc., 420 N.J. Super. 353, 21 A.3d 650 (2011), the plaintiff sued a private investigator, alleging that the investigator had invaded his privacy by having his ex-wife place a global positioning system (GPS) in his car to track his movements. The New Jersey Superior Court, however, ruled that the plaintiff's claim of privacy invasion could not cover his movements in public areas. For a discussion, see Thomas Garry, Frank Douma and Stephen Simon, 'Intelligent Transportation Systems: Personal Data Needs and Privacy Law' (2012) Transportation Law Journal 97.[81] Gerald Friedland and Robin Sommer, 'Cybercasing the Joint: On the Privacy Implications of Geo-Tagging' Paper for Proc. USENIX Workshop on Hot Topics in Security, 2010

[81] Gerald Friedland and Robin Sommer, 'Cybercasing the Joint: On the Privacy Implications of Geo-Tagging' Paper for Proc. USENIX Workshop on Hot Topics in Security, 2010 < http://www.icsi.berkeley.edu/pubs/networking/cybercasinghotsec10.pdf> accessed 17 April 2013.

[82] Please Rob Me – Raising Awareness About Over-sharing, <http://pleaserobme.com> accessed 17 April 2013.

protection of their privacy. However, others have defined locational privacy as 'the ability of individuals to move in public space with the expectation that under normal circumstances their location will not be systematically and secretly monitored for later use.'[83] It also entails the significant issue of an individual's control over the extent of the accessibility and use of personal location information, including the sequence of locations.[84] What becomes critical in this concept of locational privacy is the reasonable and legitimate expectation of privacy that can be expected when moving in a public place. However, the development of case law is highly dependent on the context of each case, and the legal position is far from settled.[85] A more viable and speedier option, which is the subject of current debate in both Europe and the US, is to expand the definition of personal data to include location data.

A. Attempts and Legal Limits of Legal Regulations on Location Data: the EU and the US Models

1. The Regulatory Framework in the EU

In the EU, the two major governing pieces of legislation on personal data protection are the Data Protection Directive (95/46/EC)[86] and the ePrivacy Directive (2002/58/EC, as

[83] Natural Resources Canada, 'Geospatial Privacy Awareness and Risk Management Guide for Federal Agencies' 10 (31 March 2010) <http://geogratis.cgdi.gc.ca/eodata/download/part6/ess_pubs/288/288860/cgdi_ip_12.pdf> accessed 17 April 2013. Electronic Privacy Information Centre, 'Locational Privacy' <http://epic.org/privacy/location_privacy/default.html#Issues> accessed 17 April 2013.

[84] Michael and Clarke (n. 6) 220.

[85] Anne S.Y. Cheung, 'Rethinking Public Privacy in the Internet Era: A Study of Virtual Persecution by the Internet Crowd' (2009) 2 Journal of Media Law 191.

[86] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. Official Journal L 281, 23/11/1995 P. 0031 – 0050

revised in Directive 2009/136/EC) of the European Parliament and Council. [87]

(a) ePrivacy Directive

The ePrivacy Directive is of direct relevance to the issue of location data. Under paragraph 14 of the Preamble, location data

> may refer to the latitude, longitude and altitude of the user's terminal equipment, to the direction of travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time and to the time the location information was recorded.

Furthermore, under Article 2(c) of the ePrivacy Directive, location data is defined as

> any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service.

Under the above legal regime, public carriers of telecommunications services are prohibited from using traffic data for the purposes of marketing electronic communications

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML> accessed 18 April 2013.

[87] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communication Sector (Directive on Privacy and Electronic Communications), Official Journal L 201, 31/07/2002 P.0037-0047. Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, Amending Directive 2002/22/Ec on Universal Service And Users' Rights Relating to Electronic Communications Networks and Services, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector and Regulation (Ec) No 2006/2004 on Cooperation between National Authorities Responsible for the Enforcement Of Consumer Protection Laws. Official Journal of the European Union L 337/11. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:En:PDF > accessed 17 April 2013.

services or for the provision of value-added services, including location-based services for advertising purposes, without the consent of the users (Article 6(3)).[88] In addition, location data must be made anonymous by the public carriers, or specific types of notice must be given to and consent must be obtained from the users, before any processing of personal data (Article 9). Users must also be given the opportunity to withdraw their consent at any time (Article 9). Another important point to note is that when an entity (whether public or private, an individual programmer, major corporation, data controller, data processor or third party) places information on or reads information from the terminal equipment of a user, clear and comprehensive information must be given and consent must be obtained from the user under Article 5(3) of the ePrivacy Directive.[89] This means that any entity that places information on or reads information from smart devices, including apps, must obtain prior consent.[90] This consent arguably covers not only the collection or use of personal data, but also any information that is being stored or accessed by the entity.[91]

---

[88] Nancy J King and Pernille Wegener Jessen, 'Profiling the Mobile Customer – Privacy Concerns when Behavioural Advertisers Target Mobile Phones – Part I' (2010) 26 Computer Law & Security Review 455, 464-5.

[89] Article 5(3) of the ePrivacy Directive stipulates that 'Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.'

[90] Article 29 Data Protection Working Party, 'Opinion 02/2013 on Apps on Smart Devices' (adopted 27 February 2013) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf> paragraph 3.1, accessed 17 April 2013.

[91] *Ibid*. This interpretation of Article 29 Working Party has raised concerns for creating cumbersome burden on the industry that may inhibit growth and innovation in the mobile app industry in Europe. Saira Nayak, 'Response to EU Opinion on Mobile Apps' Truste Blog, 14 March 2014

Despite the above seemingly adequate protection given to users regarding the use of location data by third parties in the EU, the ePrivacy Directive binds only public electronic communication services and networks (telecom operators) (Article 2). In other words, in the context of regulating the processing of location data in relation to geo-location technologies, the ePrivacy Directive applies only to the processing of base station data by public telecommunications service providers, and by those telecom operators that offer hybrid geo-location services based on the processing of other types of location data, including GPS or WiFi data.[92]

Companies that are defined as 'information society services' are excluded from the above legal framework.[93] Hence, when a user chooses to transmit GPS data over the Internet, the telecommunication service provider is merely acting as a conduit, as the GPS signal is

---

<http://www.truste.com/blog/2013/03/14/response-to-eu-opinion-on-mobile-apps/> accessed 17 April 2013.

[92] Article 29 Data Protection Working Party, 'Opinion 13/2011 on Geolocation Services on Smart Mobile Devices' (adopted 16 May 2011) <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf>, paragraph 4.1 accessed 17 April 2013. For a discussion of an alternative non-legal techno-regulatory regime, see Bibi van den Berg, and Ronald E. Leenes, 'Abort, Retry, Fail: Scoping Techno-Regulation and other Techno-effects' in M. Hildbrandt and A.M.P. Gaakeer, eds., *Human Law and Computer Law: Comparative Perspectives* (Dordrecht, Heidelberg: Springer, 2013) 67-87.

[93] Under Article 2(c) of Directive 2002/21/EC, an 'electronic communications service' is defined as a service normally provided for remuneration, which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services on networks used for broadcasting, but excluding services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks. DIRECTIVE 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a Common Regulatory Framework For Electronic Communications Networks And Services (Framework Directive). Official Journal of the European Communities L 108/33. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0033:0033:EN:PDF> accessed 17 April 2013.

transmitted at the application level of Internet communication.[94] Following this framework, web-based LBS providers and companies that provide location services and applications based on GPS and WiFi data may fall outside the regulatory framework of the ePrivacy Directive. Cuijpers and Pekarek rightly criticise that the aforesaid distinction between public and private networks has become diffused and causes confusion to the regulatory framework.[95]

(b) Data Protection Directive

Even if the ePrivacy Directive may not be applicable to every case of location data protection, the Data Protection Directive can provide a fall-back. The latter carries specific provisions related to the processing of personal data, covering the collection, retention, use and disclosure of data, among other aspects. Under the Data Protection Directive, personal data refers to 'any information relating to an identified or identifiable natural person', including those that 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'. Recalling our earlier definition of location data (mentioned in Part IA) as 'any data which places one at a particular location at any given point in time, or at a series of locations over time', it is only logical to conclude that location

[94] Article 29 Data Protection Working Party, above n. 92, para 4.2.1.
[95] Colette Cuijpers and Martin Pekarek, 'The Regulation of Location-Based Services: The Challenges to the European Union Data Protection Regime' 5 Journal of Location Based Services (2011) 223, 230.

data form part of personal data.

This stance is also consistent with the position of Article 29 of the Data Protection Working Party on why location data should be considered as personal data under the EU regime.[96] First, the Article 29 Group points out that location data are linked directly to a person because the telecom operator that provides the global system for mobiles (GSM) and mobile Internet access has a record of the name, address and banking details of every customer. Second, location data are also linked indirectly but inextricably to the users of mobile devices through a combination of the unique numbers associated with each device, such as the IMEI and the MAC address of smart mobile devices.[97] If the above arguments are accepted, prior informed and specific consent must be sought from users before such data can be collected and processed (Articles 7-10 of the Data Protection Directive).

(c) Proposed General Data Protection Regulation

The above debate on whether location data should be regarded as personal data may be

[96] The Article 29 Working Party was set up under article 29 of the EU Data Protection Directive. It is composed of representatives from the EU member states' data protection authorities, the European Data Protection Supervisor and the European Commission. *Ibid*, para 4.2.2.

[97] *Ibid*. IMEI stands for International Mobile Equipment Identity number. It is a 15-digit number that uniquely identifies the device on the cellular network. IMEIs are primarily useful for tracking stolen devices, and are often re-purposed as user IDs in mobile applications. In 2011, Website security company Dasient found examples of PC-based tracking techniques getting extended in a troublesome way to Internet-connected mobile devices. It analysed 10,000 free mobile apps that enable gaming, financial services, entertainment and other services on Google Android smartphones, and found that more than 8%, or 842, of the Android apps took the unusual step of asking users' permission to access the handset's IMEI number. The IMEI was then employed as the user ID for the given app. In a number of instances, the app subsequently forwarded the user's IMEI on to an online advertising network. Dasient Blog, 'Hashing IMEI Numbers Does Not Protect Privacy' (26 July 2011) <http://blog.dasient.com/2011/07/hashing-imei-numbers-does-not-protect.html> accessed 5 September 2013.

readily resolved if the General Data Protection Regulation (hereinafter referred to as the Regulation) proposed by the European Commission is adopted in the near future. [98] In January 2012, the European Commission announced a comprehensive set of reforms on data protection. One important proposal was to replace the Data Protection Directive with the Regulation.[99] Under Article 4 of the proposed Regulation, the meaning of 'personal data' is simplified to mean 'any information relating to a data subject'. The meaning of 'data subject' is amended to

> an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifiers or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Privacy experts have welcomed the proposed changes.[100] Costa and Poullet argue that the current definition of personal data under the Data Protection Directive is heavily dependent on 'nominative identification';[101] that is, whether one person can be distinguished from others by reference to personally identifying information such as identification numbers,

---

[98] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)' 25 January 2012, < http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf > accessed 17 April 2013.

[99] Luiz Costa and Yves Poullet, 'Privacy and the Regulation of 2012' (2012) 28 Computer Law & Security Review 254.

[100] *Ibid*.

[101] *Ibid*, 255.

names, addresses and health and financial data. Yet they forcefully argue out that the advancement of modern technology allows the contacting, profiling and identification of individuals without any need to resort to any of the nominative data.[102] For instance, profiling technology enables consumers to be identified individually based on their browsing behaviour, purchasing habits and the geographic location data generated by their mobile devices.[103] In the specific context of location data, studies by computer scientists have also shown that individuals can be identified easily from anonymised or aggregated data sets because human mobility patterns are largely predictable and non-random.[104] Given the large amount of information that can be inferred from location data, this finding has important implications for personal data and privacy protection. In light of the above, the expanded definition of personal data under the proposed Regulation as 'any information relating to a data subject' is indeed most sensible.

Under the proposed Regulation, personal data must be 'processed lawfully, fairly and in a transparent manner in relation to the data subject' (Article 5a). Although clearer guidelines are needed on what specific information must be given to data subjects to satisfy the

[102] *Ibid*.
[103] King and Jessen (n. 88) 458.
[104] Computer scientists at Massachusetts Institute of Technology and the Catholic University of Louvain studied 15 months' worth of anonymised mobile phone records for 1.5 million individuals, and found that four location and time points were enough to accurately identify 95% of the subjects studied. Yves-Alexandre de Montjoye et al, 'Unique in the Crowd: The Privacy Bounds of Human Mobility' (2013) 3:1376 Scientific Reports 1 <http://www.nature.com/srep/2013/130325/srep01376/pdf/srep01376.pdf> accessed 19 April 2013. An earlier study involving one participant in Australia in 2006 reached the same conclusion. K. Michael, A. McNamee, M. G. Michael, and H. Tootell, 'Location-Based Intelligence – Modeling Behavior in Humans using GPS' IEEE International Symposium on Technology and Society. New York, United States: IEEE, 2006
< http://works.bepress.com/kmichael/6> accessed 28 August 2013.

requirement of 'transparency', the proposed model is moving in the right direction of vesting more control back to the users and granting them genuine choices over the use of their location data.

2. The US Regulatory Framework

(a) Federal Law

In contrast to the EU model, there is no federal law in the US that addresses the specific problem of location data or regulates the use of geo-location technologies to protect consumers.[105] The two principal pieces of legislation covering the commercial industry are the Communications Act and the Electronic Communications Privacy Act. However, both of these are limited in scope due to the specific carriers that they aim to regulate.

(1) The Communications Act: CPNI

Arguably, the consumer proprietary network information (CPNI) rules of S. 222 of the Communications Act (also known as the Telecommunications Act of 1996) protect location

[105] For the legal position on the state's authority to use location information and to use tracking devices at both the federal and state levels, see Rainey Reitman, 'New Bill Would Ensure Law Enforcement Gets a Warrant Before Reading Email', *Electronic Frontier Foundation*, 8 March 2013 <https://www.eff.org/deeplinks/2013/03/new-bill-would-ensure-law-enforcement-get-warrant-reading-email> accessed 20 April 2013. 'Locational Privacy' Electronic Privacy Information Center <http://epic.org/privacy/location_privacy/>accessed 20 April 2013. For the implications of the First Amendment and the Fourth Amendment on surveillance and location data, see Andrew Crocker, 'Trackers that Make Phone Calls: Considering First Amendment Protection for Location Data' 26:2 Harvard Journal of Law & Technology (2013) <http://jolt.law.harvard.edu/articles/pdf/v26/26HarvJLTech619.pdf> accessed 10 September 2013.

information.[106] This is because under S. 222(f), telecom carriers must obtain express consent from consumers before they can disclose location information to any third party, except in emergency situations.[107] However, like the e-Privacy Directive in Europe, the CPNI rules only bind telecommunications carriers and providers of interconnected VoIP service.[108] This renders technologies that determine a person's location independent of the carrier, such as Wi-Fi and apps, outside the scope of the regulation.

Furthermore, in the case of *US West Inc. v. FCC*,[109] the federal district court held that telephone records held by a telecom carrier are protected commercial speech under the First Amendment, for which consent could be obtained in an opt-out regime. Applying this case to the present context may mean that carriers do not need to obtain express opt-in consent from customers to share their location data or use it for marketing purposes. This position is woefully inadequate for protecting users' location data because many users, as explained above, are not aware that they or their devices are being mapped, tracked or tagged.

Finally, even when a telecommunications carrier is involved in providing LBS, CPNI

---

[106] CPNI refers to (A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier. 47 U.S.C. § 222(h)(1).

[107] The relevant provisions under S. 222 of the Telecommunications Act governing location data and the exception in emergency is also known as the Wireless Communication and Public Safety Act of 1999 or E911 Act. *Federal Communications Commission, In the Matter of Request by Cellular Telecommunications and Internet Association to Commence Rulemaking to Establish Fair Location Information Practices* (WT Docket No. 01-72, 200), <http://epic.org/privacy/wireless/FCC_order.pdf> accessed 17 April 2013.

[108] Federal Communications Commission, In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information IP-Enabled Services FCC 07-22 (2007) 2 note 3 <http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-22A1.pdf> accessed 17 April 2013.

[109] 182 F.3d 1224 (10th Cir. 1999), cert. denied, 120 S.Ct. 2215 (2000).

rules may not apply because the Federal Communications Commission has refrained from applying Title II of the Communications Act, including the CPNI rules, to wireless broadband services.[110]

(2) Electronic Communications Privacy Act

Likewise, the scope of the federal Electronic Communications Privacy Act (ECPA) suffers from the same problem of being overly dependent on the forms of providers to be regulated.[111] The ECPA was enacted in 1986 before the age of the Internet and the widespread use of geo-location technologies. Although Title II (§2701- §2712, also known as the Stored Communications Act) of the ECPA protects the privacy of consumers,[112] its scope only covers providers of electronic communications services and providers of remote computing services.[113] The aim of the statute is to protect the communication privacy of customers in the form of electronic storage, defined as 'any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof'.[114]

[110] Federal Communications Commission, Legal Framework, <http://www.broadband.gov/legal-framework-glossary.html> accessed 17 April 2013. For a discussion, see Center for Democracy and Technology, 'CDT Testifies on Location Privacy' (2 March 2010) <https://www.cdt.org/policy/cdt-testifies-location-privacy> accessed 17 April 2013.
[111] 18 U.S.C.
[112] US Department of Justice, Justice Information Sharing: Privacy and Civil Liberties, <http://it.ojp.gov/default.aspx?area=privacy&page=1285> accessed 17 April 2013.
[113] For an overview of the legislative framework, see Orin S. Kerr, 'A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It' (2004) 72 George Washington Law Review 1208.
[114] Under S. 2510 (17)(A) of the ECPA, 18 U.S.C., 'electronic storage' means
(A) any temporary, intermediate storage of a wire or electronic communication incidental to the

The focus of the statute is to protect content-based communications.[115] In contrast, under §2702(c)(6), providers are allowed to disclose non-content information to anyone,[116] including a person's name, address and communication records.

The above shortcomings of the ECPA in protecting consumers' data in today's technological society are evident in the case of *In re DoubleClick, Inc. Privacy Litigation.*[117] The dispute concerned a class action against the defendant company for placing cookies on the hard drives of users so that it could collect, compile and analyse information that enabled it to deliver targeted online advertising. It was contended that the process involved unauthorised access to data, which was against the ECPA. The New York District Court ruled that the defendant company had not violated the ECPA because the cookies were permanently installed in the plaintiffs' computers, whereas the ECPA restricted unauthorised access only to communications in 'temporary, intermediate storage'.[118] Daniel Solove points out that the

---

electronic transmission thereof; and
(B) any storage of such communication by an electronic communication service for the purposes of backup protection of such communication.

[115] 18 U.S.C., S. 2702(a)

[116] S. 2702(c) stipulates that a 'provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2)):
(1) as otherwise authorised in section 2703;
(2) with the lawful consent of the customer or subscriber;
(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;
(4) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency;
(5) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A; or
(6) to any person other than a governmental entity.'

[117] 154 F. Supp. 2d 497.

[118] Section 2510(17) of the ECPA defines 'electronic storage' as:
'(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

decision shows that the statute is outdated and ill-tailored to address the prevalent practice of information gathering by the private sector in the Internet age.[119] Applying the same legal logic to apps installed on users' mobile devices, it is unlikely that users could claim personal data protection against unauthorised access and sharing of data.

(3) Further Limitations

Frustrated by the location privacy protection in the US under the Telecommunications Act and the ECPA, Senator Al Franken described the legal landscape as a 'confusing hodgepodge of regulation'.[120] He vividly illustrated the problem using the example of a person who uses his smartphone to place a phone call to a business, in which that person's wireless company cannot disclose his location information to a third party without his prior consent. However, when the same person uses the same phone to look up that business on the Internet, his wireless company can disclose his location to anyone without legal repercussions.[121]

Due to the lack of a clear legal regulatory stance on location privacy in the US, it is

(B) any storage of such communication by an electronic communication service for the purpose of backup protection of such communication.' In *re Doubleclick Inc. Privacy Litigation*, 154 F. Supp. 2d 497, 511.

[119] Daniel J. Solove, *The Digital Person* (New York University Press 2004) 69.

[120] Senator Al Franken, The Location Privacy Protection Act of 2011 (S. 1223) Bill Summary <http://franken.senate.gov/files/docs/110614_The_Location_Privacy_Protection_Act_of_2011_One_pager.pdf > accessed 17 April 2013.

[121] *Ibid*.

common to see a patchwork of different responses from the industry. While it is common for service providers to provide users with a choice of privacy settings, the set of options and their defaults tend to differ.[122] For example, YouTube uses geo-information from uploaded videos by default, while Flickr requires explicit opt-in.[123] Similarly, Apple's iPhone geotags all images taken with the internal camera unless the function is specifically disabled, whereas Android-based phones require users to turn the function on.[124]

Another problem is the discretionary enforcement of the law. In 2011, the US Federal Trade Commission was confronted with the first case involving the use of apps in the alleged violation of the Children's Online Privacy Protection Act.[125] It was found that W3 Innovations, through its Broken Thumbs app, had been collecting and disclosing personal information from tens of thousands of children under the age of 13 without prior consent from their parents. Eventually, the case was settled, with the company agreeing to pay a US$50,000 penalty and to delete all of the personal information, including email addresses, that they had collected from children.

(b) State Attempt: California Online Privacy Protection Act

While different states have tabled different Location Privacy Bills to establish a warrant

[122] Friedland and Sommer (n. 61), 2.
[123] *Ibid*.
[124] *Ibid*.
[125] *United States of America, Plaintiff v. W3 Innovations,* (United States District Court for the Northern District of California) (12 August 2011) Case No. CV-11-03958-PSG <http://www.ftc.gov/os/caselist/1023251/index.shtm> accessed 17 April 2013.
FTC File No. 102 3251

requirement for the authorities to use location information,[126] California remains the only state that has implemented personal information and privacy policies to protect consumers in the use of mobile applications and websites.

Under Section 22575(a) of the California Online Privacy Protection Act (CalOPPA),[127] 'an operator of a commercial Web site or online service that collects personally identifiable information through the Internet about individual consumers residing in California who use or visit its commercial Web site or online service shall conspicuously post its privacy policy on its Web site.' Under S. 22577(b), the definition of personally identifiable information is any 'individually identifiable information about an individual consumer collected online by the operator from that individual and maintained by the operator in an accessible form.'[128] Section 22577(b) meticulously elaborates what is meant by 'conspicuously posting'.

Regarding the imposition of penalties, each violation may carry a fine of up to US$2500. The CalOPPA is expected to be enforced through California's Unfair Competition Law (the 'UCL'), which is within the Business and Professions Code (ss17200-17209). Under the UCL, the California Attorney General, district attorneys and some city and county attorneys can file suits against businesses for acts of 'unfair competition', which are considered to be any act

[126] These include Texas, Maryland and California. 'Locational Privacy Electronic Privacy Information Center' <http://epic.org/privacy/location_privacy/ > accessed 20 April 2013.
[127] The Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code §§ 22575-22579 (2004). California Code - Section 22575.
[128] The various forms of identification include (1) first and last name; (2) home or other physical address, including street name and name of a city or town; (3) e-mail addresses; (4) telephone numbers; (5) social security number; (6) any other identifier that permits the physical or online contacting of a specific individual; and (7) information concerning a user that the Web site or online service collects online from the user and maintains in personally identifiable form in combination with an identifier described in this subdivision.

involving business that violates California law.

In 2012, the Attorney General Office of California brought a lawsuit against Delta Air Lines for violating the CalOPPA by failing to conspicuously post its privacy policy for Delta applications and failing to inform users what personally identifiable information was collected and how it was being used.[129] In the same year, the Attorney General also sent warning letters to about 100 mobile app operators concerning their non-compliance with the law.[130]

Although the CalOPPA is likely to cover location information, the requirements of the notification of privacy policy are relatively lax. At best, users can find out the information easily; however, they do not have the choice to opt out of the regime, let alone to express their explicit consent or objection.

(c) Proposed Reform

Legal rules have been proposed in the US in response to the uncertain and unsatisfactory state of protection on location privacy protection.

[129] Andrew Hoffman, 'California Attorney General Sues Delta Air Lines for Failing to Have a Mobile App Privacy Policy' (*Information Law Group*, 10 December 2012) <http://www.infolawgroup.com/2012/12/articles/privacy-law/california-attorney-general-sues-delta-air-lines-for-failing-to-have-a-mobile-app-privacy-policy/> accessed 20 April 2013.

[130] Hunton & Williams LLP, 'California AG Sues Delta for Failure to Post a Privacy Policy on Its Mobile App' (*Privacy and Information Security Law Blog*, 7 December 2012) <http://www.huntonprivacyblog.com/2012/12/articles/california-ag-sues-delta-for-failure-to-post-a-privacy-policy-on-its-mobile-app/> accessed 20 April 2013.

(1) Location Privacy Protection Act

In June 2011, the Location Privacy Protection Act of 2011 (S. 1223) was tabled before Congress by Senator Al Franken.[131] Under Section 2 of the bill, geo-location information is defined as any information

> concerning the location of an electronic communications device that …is generated by or derived from the operation or use of the electronic communications device; and that may be used to identify or approximate the location of the electronic communications device or the individual that is using the device,

but 'does not include any temporarily assigned network address or Internet protocol address of the individual'. The bill specifically addresses geo-location information services, defined as 'the provision of a global positioning service or other mapping, locational, or directional information service (Section 3, Clause 2713 (5)). It is intended to cover businesses offering or providing services for electronic communications devices, including those offering or providing electronic communications services, remote computing services or geo-location information services (Section 3, Clause 2713(a)(1)).[132]

The proposed legislation has three important implications for future industry practice. First, companies must obtain express consent from customers before collecting, receiving,

[131] Location Privacy Protection Act, 2011 Congress US S 1223, 112th CONGRESS, 1st Session (June 16, 2011), Introduced in Senate, <http://www.govtrack.us/congress/billtext.xpd?bill=s112-1223> accessed 17 April 2013.
[132] For discussion of the new proposal, Michael and Clarke (n. 6).

recording or obtaining their location data, and before disclosing such data to any nongovernmental third parties (Section 3, Clause 2713(5)(b)). Second, stalking apps that allow one person to track another person's whereabouts surreptitiously will be prohibited (Section 3, Clause 2713(5)(c). Third, mobile services must disclose the names of the advertising networks or other third parties with which they share consumers' locations (clause 2713(3)). The bill was approved by the Senate Judiciary Committee at the end of 2012,[133] but it is likely to take another year of debate before we know whether it will be enacted into law.

(2) Mobile Device Privacy Act

In 2012, the Mobile Device Privacy Act was introduced to Congress by Senator Edward Markey.[134] The bill specifically regulates the monitoring of activities by mobile devices: the software's capability to monitor mobile device usage must be disclosed to the user, and the user must give express consent to monitoring and other activities.

Although the proposed Act does not aim to protect location information directly, it defines 'monitoring software' as

software with the capability to monitor mobile device usage or the location of the user

[133] The bill was passed by the Senate Judiciary Committee on 14 December 2012. The legislative process can be checked, US Legislative Information, S.1223 - Location Privacy Protection Act of 2012 <http://beta.congress.gov/bill/112th-congress/senate-bill/1223> accessed 20 April 2013.

[134] Mobile Device Privacy Act, 2012 Congress US HR 6377, 112th CONGRESS, 2nd Session (12 September 2012), Introduced in Senate,
< http://beta.congress.gov/bill/112th-congress/house-bill/6377/> accessed 20 April 2013

and to transmit the information collected to another device or system, whether or not such capability is the primary function of the software or the purpose for which it is marketed (Section 7(5)).

Thus, the collection and transmission of location information is clearly covered by the Act.

The major focus of the bill is to regulate tracking activity by the industry. It requires any seller of mobile devices to disclose tracking software at the time of sale and at the time of entry into a contract (Clauses 553(1) and (2) of Title 5, United States Code, Section 2 of the bill). Express consent from consumers must be sought before any monitoring software can be activated. In addition, consumers must be told the type of monitoring software being installed, what information is being monitored and transmitted, the identity of the person or persons who will see or share the data, how the data will be used and the procedures the consumer must follow to discontinue the monitoring and collecting (Section 3 of the Bill). It would require companies to file with the Federal Trade Commission (FTC) or the Federal Communications Commission, as appropriate, a copy of the agreement under which a person receives the information regarding the disclosures required by the Act (Section 4).

Furthermore, the bill directs the FTC to promulgate regulations requiring (1) the express consent of the user before monitoring software starts to collect and transmit information and the opportunity for the user to prohibit such collection and transmission at any time; and (2) recipients of information transmitted from monitoring software to implement information

security practices regarding the treatment and protection of the information (Section 4).

Violations of the proposed law will incur penalties of US$1000 for each violation, and up to US$3000 for wilful or knowing violations (Section 6(e)). However, it is uncertain what exactly constitutes a 'violation'. For instance, if an entity has collected and transmitted a person's personal information without permission several times, it is not clear whether this would be regarded as a number of unique violations, or one single violation. Amongst other concerns, the bill is being vehemently opposed by the mobile device and app industry.[135]

Under the current atmosphere of hostile industry response and a traditional lack of protection of personal information, it is uncertain whether the two proposed bills will be passed in the US.

B. Ongoing Legal Issues

In examining the current law and proposed legal developments in the EU and the US, we note three areas that are in urgent need of reform to protect location data: (1) expanding the scope of personal data to include location data; (2) imposing responsibility on service carriers or providers that are technologically neutral; and (3) having a system of transparency and obtaining meaningful consent from consumers.

On the first issue, the recently proposed EU Regulation, which specifically protects

[135] Alex Wilhem, 'Meet the Mobile Device Privacy Act: A New Bill to Protect Mobile Consumers that is Already Causing a Stir' (*The Next Web*, 13 September 2012). <http://thenextweb.com/us/2012/09/13/meet-mobile-device-privacy-act-a-strict-new-bill-protect-mobile-consumers-already-causing-stir/> accessed 20 April 2013.

location data and adopts a broad and flexible definition of personal data as 'any information of an individual', is moving in the right direction. As discussed, location data are highly predictable, and seemingly anonymous location data can be easily traced to an individual. An inclusive definition needs to allow for future non-contemplated technological advancements to protect the highly unique nature of location data.

Second, a technologically neutral approach towards the means of transmission is critical. We have highlighted the shortcomings of the ePrivacy Directive in the EU and the federal legislation in the US, which are unnecessarily narrow due to their strict dependence on the forms of transmission or forms of providers of the concerned data. Given that laws, once passed, 'are continually eroded by exceptions built into subsequent legislation and by technical capabilities that are not contemplated,'[136] a piece of legislation is needed that is broad enough to include the present or future means of carriers and that will not be quickly out-paced by technology.

Third, both the EU and the US model fail to make clear the degree of transparency that should be disclosed to users and consumers, and the level and type of consent that is required. Transparency will entail not only informing users and consumers about the specific information being collected, how it is being used or shared and how long it is being retained, but also notifying them of any security breach. While it is acceptable to allow for exceptional

[136] Michael and Clarke (n. 6).

cases that do not require the consent of users and consumers to be obtained, such as in an emergency, affirmative opt-in consent should be sought for collecting and sharing location data. This issue of consent in different contexts certainly warrants another independent research project. Perhaps for now, it is important for us to remember that such consent must be freely given in an opt-in regime, that it cannot be bundled with other services but must be sufficiently granular at various points in time, yet it must not be unduly burdensome to the users.[137]

Conclusion

Mobile devices have never been as popular and dynamic as they are today, but our investigation into the legal protection of location data has revealed that the law is interacting weakly with modern LBS technologies. Not only is the law lagging behind such technologies, it also appears to be helpless and lost when faced with the relentless growth of smart mobile devices equipped with ever-evolving geo-mapping, tracking and tagging technologies. While users are excited about the rapid developments on the techno-highway, they may have lost sight of the personal data violations and the surveillance that are being carried out by the industry and the market. As many users are not even aware that their data are being captured or collected by the industry, they certainly have insufficient knowledge and opportunity to

[137] *Ibid*. Evelyne Beatrix Cleff, 'Implementing the Legal Criteria of Meaningful Consent in the Concept of Mobile Advertising' (2007) 23 Computer Law & Security Review 262.

give their consent. Developments in technology and our social practices in the use of location data present unique privacy concerns and challenges.

It is laudable that legal incentives have been introduced in the EU and the US to catch up with the challenges posed by geo-locational technology. Fundamentally, however, legal provisions are required that address and protect location data directly and specifically. If the core principles behind the right to privacy and personal data protection are to protect an individual's self-determination and prevent manipulation by others, we need legal intervention that requires consent to be obtained for and that protects the collection, use, disclosure and retention of geo-location data. Vigilance is needed to guard not only against state encroachment, but also against growing commercial practice.