scripted

Volume 13, Issue 2, August 2016

PRIVACY IN LOCATION-BASED SERVICES: AN INTERDISCIPLINARY APPROACH

Michael Herrmann,[1] Mireille Hildebrandt[2], Laura Tielemans,[3] Claudia Diaz[4]•

Abstract

There exists a wide variety of location-based services (LBSs) that simplify our daily life. While engaging with LBSs, we disseminate accurate location data to remote machines and thus lose control over our data. It is well known that this raises significant privacy concerns as access to accurate location data may reveal sensitive information about an individual. In this work, we investigate the privacy implications of LBSs from a joint perspective of engineering, legal and ethical disciplines. We first outline from a technical perspective how user location data is potentially being dissiminated. Second, we employ the Contextual Integrity (CI) heuristic, an ethical approach developed by Helen Nissenbaum, to establish whether and if so, how, the dissemination of location data breaches the users' privacy. Third, we show how the concept of purpose limitation (PL) helps to clarify the restrictions on the dissemination of location data from a legal perspective. Our interdisciplinary approach allows us to highlight the privacy issues of LBSs in a more comprehensive manner than singular disciplinary exercises afford, and it enables us to contribute towards a better understanding among the relevant disciplines. Additionally, our case study allows us to provide two further contributions that are of separate interest. We address the problem of competing prevailing contexts without suggesting that the ensuing incompatability of informational norms can be resolved theoretically, even though it must be resolved in practice. This ties in with the difference between a legal approach that has to align justice with legal certainty and an ethics approach that aims

---

[1] PhD student at Computer Security and Industrial Cryptography (COSIC) at KU Leuven, iMinds.

[2] Professor at Research Group on Law, Science, Technology and Society (LSTS), Vrije Universiteit Brussel; Professor of Smart Environments, Data Protection and the Rule of Law at institute of Computing and Information Sciences (iCIS), Radboud University Nijmegen.

[3] PhD candidate at Research Group on Law, Science, Technology and Society (LSTS), Vrije Universiteit Brussel, Belgium; Lawyer at White & Case Brussels, Belgium.

[4] Professor at Computer Security and Industrial Cryptography (COSIC) at KU Leuven, iMinds.

• The research for this article was funded by the Research Foundation – Flanders (FWO) for the 4-year interdisciplinary research project on 'Contextual privacy and the proliferation of location data'.

to align prevailing social norms with moral reasoning. In the end, our interdisciplinary research shows how CI and PL are in many ways complementary.

10.2966/scrip.130216.144

1. Introduction

During the last decades, interdisciplinary research has gained significant popularity. While scholars typically work in their own self-contained and isolated domain within their community of experts, we refer to interdisciplinary research as that which brings together approaches of at least two different disciplines.

In this work, we report on our interdisciplinary research on the protection of location data. We tackle the problem from an engineering, legal, and ethical disciplinary perspective. While there are several reasons why interdisciplinary research can be fruitful,[1] we think interdisciplinary research is particularly useful for matters regarding data protection. In order to understand how data is created, transmitted and processed, one needs an understanding of technical systems, i.e. from the perspective of engineering. Yet, data processing is not merely a matter of technical possibilities, but also one of legal regulation. Hence one needs knowledge from the legal domain. Finally, we use Helen Nissenbaum's Contextual Integrity (CI) heuristic,[2] based on an ethical approach, as a middle ground between legal and technical assessments of privacy violations.

People use their smart devices, with their positioning capabilities, to engage in a wide variety of location-based services (LBSs). These services have in common that users must share their current whereabouts with a service provider to, for example, find nearby points of interest, share location data with friends, or get directions. It is well known that the ensuing mass dissemination of location data generates significant privacy concerns because location data reveals information about users that is potentially sensitive, difficult to anonymise,[3] and entities with access to accurate location data are able to make inferences about, for example, home/work address, income level, religious beliefs, sexual preferences or health issues.[4] To make things worse, behind the scenes, users share their location data with many more entities than they may be aware of and their location data may be used for purposes that they would never anticipate. This is mainly due to the current business model of many LBSs. In the case of free services, service providers finance their service by either adding third party advertisers to their applications or by selling user data to data brokers.[5] Note that LBSs thus collect location data that is not necessary to deliver their service.[6]

---

[1] For a more complete assessment on the positive impact of interdisciplinary research, please refer to M Nissani, "Ten Cheers for Interdisciplinarity: The Case for Interdisciplinary Knowledge and Research" (1997) 34 *The Social Science Journal* 201-216.

[2] H Nissenbaum *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press, 2009); H Nissenbaum, "Respecting Context to Protect Privacy: Why Meaning Matters" (2015) *Science and Engineering Ethics* 1–22.

[3] P Golle and K Partridge, "On the Anonymity of Home/Work Location Pairs" (2009) *Pervasive Computing* 390-397.

[4] M Gasson et al., "Normality Mining: Privacy Implications of Behavioral Profiles Drawn from GPS Enabled Mobile Phones" (2011) 41 *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Review* 251-261.

[5] C Timberg, "Brokers use 'billions' of data points to profile Americans" (2014) available at http://www.washingtonpost.com/business/technology/brokers-use-billions-of-data-points-to-profile-americans/2014/05/27/b4207b96-e5b2-11e3-a86b-362fd5443d19_story.html (accessed 7 July 2016).

This work is, to the best of our knowledge, the first that tackles the protection of location data from an engineering, ethical and legal perspective. From an interdisciplinary perspective, our article has four main contributions: first, the technical detail from an engineering perspective provides a substantive added value in connection with the ethical as well as the legal discipline. Second, our article serves as a reference for scholars of the involved disciplines to learn how the issue is addressed in the other two disciplines. Third, we identify a special relation between the ethical and the legal discipline, i.e. the connection between the concept of contextual integrity and purpose limitation. Fourth, our article serves as a case study on how to do interdisciplinary investigations of a data privacy matter. Additional to these interdisciplinary contributions, our work also provides valuable contributions to the CI heuristic and to the connection between the CI heuristic and data protection law. We show how the CI heuristic can be applied in a way that sensitises readers (and users) to what is at stake, and clarifies what the heuristic adds to the commonly stated opinion that location data can be sensitive data. Finally, our article discusses the legal concept of purpose limitation with respect to location data and argues its added value compared to contextual integrity.

Many of the terms used in this work have a precise meaning within one discipline, while evoking less precise connotations within the "other" discipline. For instance, in legal terms, sensitive data refers to a specific category of data, summed up in art. 8 of the Data Protection Directive (DPD) and in art. 9 of the General Data Protection Regulation (GDPR) that will replace the DPR from May 2018.[7] This concerns personal data revealing, among other things, ethnic or racial origin, or political beliefs. Being qualified as sensitive data has legal effect, since the processing of such data is by default prohibited. Location data is not sensitive data in this sense, though individuals may perceive their location to reveal sensitive information in a more general sense, and when correlated with other data location data may indeed result in data that is "sensitive" in the sense of EU data protection law. Since this article is co-authored by computer engineers and lawyers, we refer to sensitive data in the general sense of the term and will specify when we use the term in the legal sense. Other examples of potential misunderstandings may arise, for instance, when engineers speak of "users", "clients", and "service providers", whereas lawyers speak of "data subjects" and "data controllers. This is important because legal terms have legal effect and must therefore be used with precision. By specifying the legal meaning whenever

---

Under EU law this would probably be prohibited, though admittedly enforcement is lacking. For more information on the practice of data brokers: Federal Trade Commission, "A Call for Transparency and Accountability" available at http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf (accessed 7 July 2016).

[6] Under EU law this is prohibited ex art. 6 DPD, unless the data are processed for a compatible purpose and a valid legal ground is applicable. Under US law such general restrictions do not apply, therefore US companies are less concerned about re-use of personal data.

[7] 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 [1995] OJ L281/31 (Data Protection Directive (DPD)), and Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation (GDPR)). Art. 99.2 GDPR stipulates that it will apply in the Member States of the EU from 18th May 2018.

relevant, we aim to contribute to the necessary dialogue between both disciplines on the challenges and solutions regarding the proliferation of location data.

2. Location-based Services

2.1 Overview

With LBSs, we commonly refer to services that take the user's current or past location as input to provide a service. Enabled by the mass usage of mobile devices with positioning capacities, LBSs have become very popular over the last decade.[8] Today, there is a wide variety of LBSs. Google Maps is arguably the most popular and most commonly used LBS. It allows users to get directions to almost any possible place and thus became a companion on most smartphones. Other highly popular LBSs are services such as geo-social networks (GSNs), where users share information about their current whereabouts in the form of a check-in and as a way to maintain their social network. Foursquare, one of the best-known GSNs, allows users to check into venues, leave comments, share their activity with their friends, and obtain rewards for their system usage. Although they also have a strong focus on social interaction, applications such as Highlight are different from applications such as Foursquare since their focus is rather on displaying publicly available information on people in close proximity.[9] Other examples of LBSs include applications for directions in a city's public transport[10] and even Twitter, which has a functionality for adding location tags to one's tweets.

2.2 The Business Model of Location-based Services

Many LBSs are free to use[11] and although user data monetisation is not necessarily limited to free applications, such applications aim to monetise the information their providers gain about the users. This can be either information the users intentionally or unintentionally share while engaging with the LBS, or data the LBS learns by observing the user's activities. More importantly, monetisation may depend on inferences drawn from the data, possibly combined with data from other sources (Facebook, for instance, has contracts with large data brokers).[12]

2.3 Involved Parties

In the technical literature, a so-called "adversary" is everyone that may observe the user's location data. In the following, as a preparation for applying the CI heuristic,

---

[8] 49% of all users possessing a smart phone use LBS according to M Duggan, "Cell Phone Activities 2013" available at http://pewinternet.org/Reports/2013/Cell-Activities.aspx (accessed 8 July 2016)

[9] Other such services are for example: Sonar, Banjo and Kismet.

[10] Examples include OBB Scotty, Visit Paris by Metro, Tube Map London Underground.

[11] Exceptions are for example: C2G (carpooling), Caches (Geo-Caching), MeetupGroup (group meeting).

[12] K Hill, "Facebook Joins Forces With Data Brokers To Gather More Intel About Users For Ads" available at http://www.forbes.com/sites/kashmirhill/2013/02/27/facebook-joins-forces-with-data-brokers-to-gather-more-intel-about-users-for-ads/ (accessed 8 July 2016).

we elaborate on the most common entities that may observe user location data. With *user* we refer to the human engaging with an LBS by means of a *mobile device* (MD). The mobile device may be any piece of hardware manufactured by a *hardware manufacturer* (HM), such as a smart phone or tablet computer, which is able to determine its current location. On the software side, the mobile device may run software developed by multiple parties. The *operating system* (OS) is the software that is loaded on the mobile device when powered on. The *operating system manufacturer* (OSM) may be different from the HM of the mobile device. However, the HM may have modified the operating system in order to run its own services on the MD. Usually, the OS allows the user to download and install *mobile applications* (MA), which have been developed by a *mobile application developer* (MAD). The MA usually consists of the program written by the MAD - the *core-application* - but may also include third party software (TPS) written by a *third party software developer* (TPSD). To summarise, a user's mobile device may run software provided by the following parties: the HM, OSM, MAD and TPSD. Along with common terminology, we use the term LBS to refer to the combined software of the MAD and the TPSD, and use the terms core-application and TPS only if we need to refer to this separately. The data that is sent and received by a mobile device is usually transferred by one or several network operators (NO). Depending on how the MA or TPS is implemented, the NO has access to the user's data in encrypted or unencrypted form. Finally, Government entities (Gv), such as law enforcement agencies, tax authorities or intelligence agencies, may be able to obtain access to the user's data by means of warrants that allow for eavesdropping or hacking.[13]

Table 1: Summary of the involved parties.

Entity	Acronym	Description
Mobile Device	MD	Smart phone or tablet computer with positioning capabilities
Hardware Manufacturer	HM	Company that manufactures MDs such as Samsung or Apple
Operating System	OS	Software which enables the usage of the hardware by MAs
Operating System Manufacturer	OSM	Company that developed the OS
Mobile Application	MA	Software that runs on top of the OS
Mobile Application Developer	MAD	Company that developed the MA
core-application		Software developed by the MAD
Third Party Software	TPS	Any additional software that is integrated with the MA
Third Party Software Developer	TPSD	Company that developed the TPS

[13] A Landau "Making sense from Snowden: What's significant in the NSA surveillance revelations" (2013) 4 *IEEE Security & Privacy* 54-63.

Location-based Service	LBS	Service that utilises the geo location of users consisting of core-application and TPS.
Location-based Service Provider	LBSP	Legal and technical entity running the LBS
Network Operator	NO	Company that runs the physical communication infrastructure
Government	Gv	Any governmental institution with legal right to access companies databases or communication infrastructure?

3. Introducing the Contextual Integrity (CI) Heuristic

Contextual integrity (CI) is a concept introduced by Helen Nissenbaum to better understand what is at stake with privacy and to uncover the issues that can arise when sharing data. In her book, *Privacy in Context*,[14] Nissenbaum introduces the CI decision heuristic as a tool to determine whether a new socio-technical practice violates informational norms and thereby infringes privacy. The CI heuristic considers the interplay between context, roles, actors, attributes, values, informational norms, and transmission principles. The key idea of this framework is that information flows between people, and between people and other entities, occur in a specific context, taking note that this context implies specific informational norms and transmission principles. Such norms and principles may, for instance, determine how the exchanged information can be further disseminated. Specifically, user privacy is breached if information is shared in disregard for a transmission principle implied in the context where the information was first shared. For example, in the context of professional advice, where a client might share information with her lawyer, one of the transmission principles will be that the information is confidential. If the lawyer shares this information with the client's colleagues, the contextual integrity would be violated, because the transmission principle under which the information was first exchanged does not foresee a further information flow from the lawyer to such others.

The framework of contextual integrity refines the predictability of informational flows and privacy expectations; it is not so much the average or the "general" behaviour of people that will create these expectations, but rather the normative framework that shapes what is considered as "reasonably expectable". CI is not about the regularity of behaviour but about legitimate expectations. The importance attached to existing informational norms and transmission principles may be qualified as conservative. However, the point of CI is not that informational norms should not change, but that such change should be determined by those sharing a context and not imposed by socio-technical innovations. So, even if the CI heuristic can be qualified as conservative in some respects, it acknowledges that rapid technological developments may have advantages for society that justify change. This entails that emerging socio-technical practices may allow for new informational norms that challenge and reconfigure contextual integrity. However, not anything goes, and such reconfiguration requires careful deliberation. Based on this, those concerned may

[14] H Nissenbaum *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Palo Alto: Stanford University Press, 2009).

come to the conclusion that these new informational norms actually benefit society. This, however, necessitates appropriate safeguards to prevent, reduce and/or compensate the potential harm for those that suffer the consequences of newly distributed information flows.

The CI heuristic includes nine steps that we briefly outline in the following:

1. Describe the new socio-technical practice in terms of information flows.
2. Identify the prevailing context of the new practice.
3. Add general information about the sender, receiver and referent that are part of the practice.
4. Identify the transmission principles of the prevailing context.
5. Identify applicable entrenched informational norms.
6. Conduct a *prima facie* assessment on whether contextual integrity is breached by analysing the results of the previous steps and by observing whether entrenched norms have been violated.
7. Investigate what harms or threats to autonomy, freedom, power structures, justice, fairness, equality, social hierarchy and democracy are implicated by the new socio-technical practices.
8. Analyse how the practices directly impinge on values, goals, and ends of the identified context.
9. Conclude the CI heuristic and analyse whether the violation of entrenched norms is justified by the benefits of the new practice for the society, considering the fact that harms and benefits may be distributed in ways that disadvantage parties that are already disadvantaged.

4. Applying the CI Heuristic

4.1 Choosing a Context: Gateway or Vanishing Point

In the following, we employ Nissenbaum's contextual integrity (CI) heuristic for the socio-technical practice of LBSs. A key challenge is the identification of the prevailing context, required in step 2. In a sense, the choice of the relevant context is the gateway as well as the vanishing point of the entire exercise. The idea behind contextual integrity is that privacy cannot be determined in general, but depends on the context. In her book, Nissenbaum discusses a series of specific contexts, which enable an investigation of relevant information flows in a great level of detail and a concrete evaluation of specified scenarios.

The usage of MDs and MAs has become ubiquitous in our daily life and therefore users engage with LBSs in many different situations. Each situation involves various contexts, e.g. checking into a favourite café during a work break (leisure, work); getting directions during weekend trips (holidays, leisure); searching for a restaurant while being in an unfamiliar city during a business trip (business, leisure). Instead of discussing all the possible contexts, we identify the context of *travel* as the prevailing context of people engaging with LBSs. Since "travel" can be subdivided into business (or other work-related) travel, leisure travel (holiday) and migration (including illegal

immigration), we will focus on business and leisure, as migration entails a very different set of informational norms and transmission principles.

Our analysis can be seen as a case study that should sensitise readers (and users) to the privacy risks of LBSs, showing what the heuristic adds to general statements that qualify location data as sensitive data.

4.2 Socio-technical Practice in Terms of Information Flow

The first step of the CI heuristic requires us to explain how a new socio-technical practice impacts information flows by either changing existing ones or by generating new ones. We will analyse the information flows of LBSs under the third step, when discussing the participants that exchange information. Here we discuss information flows in terms of three types of personal data, as described by the World Economy Forum (WEF): as volunteered, observed or inferred data. *Volunteered data* is data that an individual deliberately shares and transmits over a communication network, for example postings, credit card details or photographs. In the process of sharing volunteered data, additional data are captured by service providers and third parties, often without the user being aware of that collection, even if she has provided consent for this by, for example, agreeing to the terms of service. This additional data is referred to as *observed data*. Observed data often consists of behavioural data, such as clickstream or location data. Finally, *inferred data* is the output of data analysis, which can be based on either volunteered or observed data or both.

For a proper understanding of inferred data, we refer to Hildebrandt, who introduces the notion of Big Data Space (BDS) to explain the complexity of the influences of inferred data, due to the fact that "[…] databases are fused or matched, while the knowledge that is inferred can be stored, sold and re-used in other databases".[15] When third parties that the user is unaware of observe volunteered data, that volunteered data may also be considered as observed data as will behavioural data, which may be similarly observed by parties the user is not at all aware of. We therefore emphasise that a crucial aspect of the concept of inferred data is that it is difficult, if not impossible, to foresee how volunteered and observed data are used to create inferred data. In line with that, we note that data that is observed while a person is using the LBS may be combined with data from other sources, for example, with data revealed in one of her online social network profiles or data stored with data brokers. Indeed, inferred information usually serves to learn more details about a user. This may be for the purpose of personalisation or advertising and we thus argue that inferred information typically includes interests, habits and, for instance, income level or health risks of an individual person, based on how her behaviour matches inferred profiles mined from Big Data Space.

4.3 Identifying Prevailing Context

We observe that the context of travel is naturally related to the usage of LBSs, because traveling includes a person's journey, stay and departure from certain

---

[15] M Hildebrandt, "Location Data, Purpose Binding and Contextual Integrity: What's the Message?" (2014) in L Floridi (ed) *Protection of Information and the Right to Privacy-A New Equilibrium?* Law, Governance and Technology Series, vol. 17, (Springer; Dordrecht) 31-62, at 35.

locations, which may be known, anticipated or inferred by other people, companies, governments and computing systems. Furthermore, choosing the context of travel nicely illustrates the fact that users employ LBSs while being busy with all kinds of activities, which implies that they are probably engaged in different contexts at the same time. For example, a check-in during a business meeting is part of a business context, but the check-in is also definitely an action that is engaged in the user's travel context, as a person must travel to reach the location of the meeting.

In the Western world, people tend to take freedom of movement within and between countries for granted. EU citizens, for instance, probably assume that one does not require permission for moving from one place to another within the EU, and expect that no questions will be asked when doing so. Similarly, they may think that they have a right to travel unmonitored from surveillance. This shows what Western people expect in terms of informational norms and transmission principles. Arguably, specific forms of transport, such as traveling by air, are monitored more closely than other types of transport. This is related to the potential for terrorist attacks or illegal immigration. Within the EU, the expectations around freedom of movement are tested in times of terrorist suicide attacks and mass immigration following the crisis in the Middle East. Although we focus on the subcontext of leisure (and business travel), informational norms and transmission principles, in the context of such travel, will be challenged by threats to public security. This implies that the context of public security may overlap with that of travel, which highlights that the choice of the prevailing context has major implications for the outcome of the heuristic. In section 5, we will return to this point.

4.4 Identifying Sender, Receiver and Referent

We consider two cases for the identification of the sender, receiver and referent of information flows in LBSs. The first case illustrates the sender, receiver and referent from the perspective of a normal user, whereas the second case illustrates what is going on "behind the scenes". The key difference is that in the first case, the Location-based Service Provider (LBSP) is seen as a data processor that operates to serve the user, whereas in the second case, the LBSP, along with other entities, turns out to be a data controller that is processing the data for their own benefit.

Figure 1 shows the functionality of an LBS from the normal user's perspective. First, user A sends a request to the LBS, revealing information that is necessary to obtain the service and additional implicit information. For LBSs such as Google Maps, the LBSP replies to the request, while storing and analysing the received (and observed) data "to further improve its service". For LBSs such as Foursquare or Highlight, the LBSP may additionally send location data of user A to other users of the LBS. In such a case, the user typically defines the set of intended receivers.

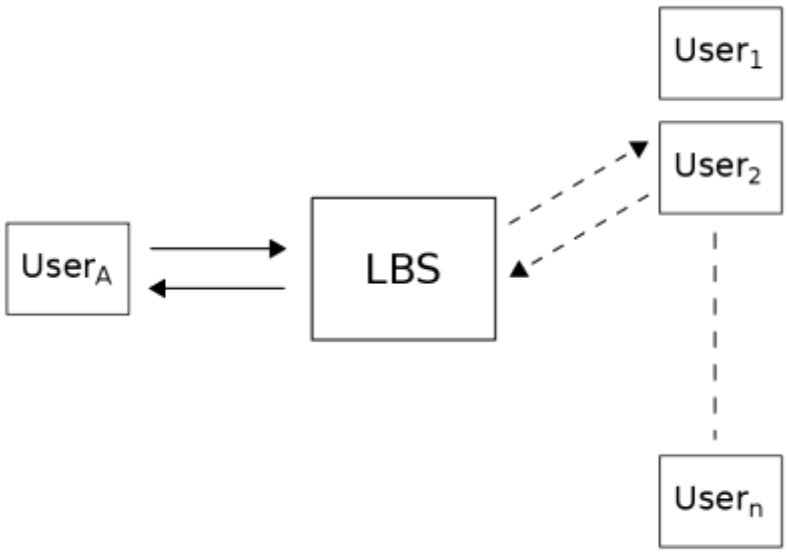

Figure 1: LBSP from a normal user's perspective (user is data controller).

Figure 2 illustrates the more comprehensive setting of how location data is disseminated in LBSs. There are two major differences to the previous case: First, we now understand that, besides the LBSP, all other entities that run software on the MD, such as the TPSD or the OSM, may access the user's location data.[16] Second, we note that location data is not only transmitted when the user actively uses the LBS, such as during a Foursquare check-in, but may also be accessed while the LBS is running in the background. In the latter case as the information flow is not intentionally sent by the user, the receiving party can be seen as the sender (it actually sends the information from the sender's device or application to itself).

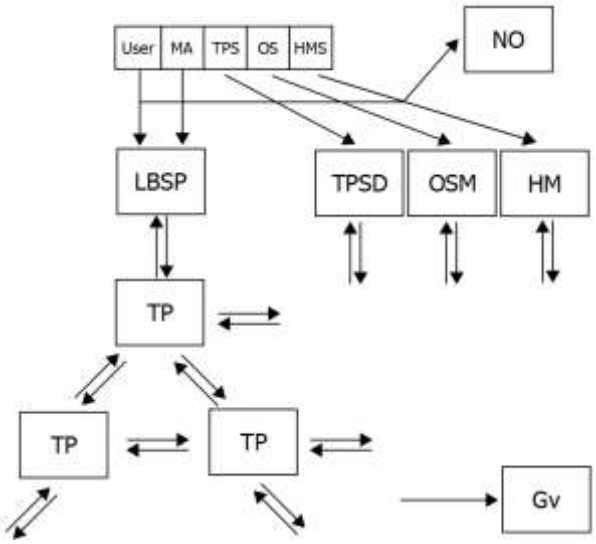

Figure 2: Overview of entities potentially learning a user's location data (user is not data controller).

[16] T Book et al, "Longitudinal analysis of android ad library permissions" (2013) *arXiv preprint arXiv:1303.0857* 1-9.

While there is enough evidence that sensitive data is transmitted from smart devices to remote destinations,[17] there is little knowledge on how the different entities depicted in Figure 2 utilise the user's location data. The LBSP, TPSD, OSM and HM may use the data (possibly (pseudo)anonymised) to optimise and personalise their services, to combine it with other data from their services,[18] or to sell the data to other third parties such as data brokers or advertising networks. Data brokers collect, aggregate and infer information from big data, while online advertising networks monetise users' behavioural data via targeted advertisements.[19] Two further entities may receive location data of users engaging with LBSs. First, the network provider (NP) since it is the provider of the communication infrastructure. Secondly, the government (Gv) since it may gain access to the data via traffic eavesdropping,[20] or by obtaining access to the LBSP's databases through the application of a warrant, or by hacking, or even simply by using the service themselves.[21]

Finally, Figure 3 illustrates that there is an actual information flow back to the user. This may be in the form of online advertisements or service personalisation that are based on the profile that has been created about the user. Location data is one of the few cases where we have evidence that it is being used for the creation of such a user profile.[22] But these profiles do not necessarily imply an information flow back to the user as they may also be used to exclude an individual from a service, premium, from employment, education or simply from access to a building or compound. Similarly, police intelligence increasingly employs location data for crime mapping, thus targeting individuals based on their location at so-called "hot spots".

---

[17] X Wei et al, "ProfileDroid: Multi-Layer Profiling of Android Applications" (2012) *Proceedings of the 18th Annual International Conference on Mobile Computing and Networking*.

[18] From a legal perspective any such processing requires of a legal ground and a specific, explicit and legitimate purpose that restricts the use of personal data. However, before discussing the legal constraints, we check what is technically possible and feasible in view of current business models.

[19] L Olejnik et al, "Selling off Privacy at Auction" (2014) *Network & Distributed System Symposium* 1-15.

[20] M Lee, "Secret 'BADASS' Intelligence Program Spied on Smartphones" available at https://theintercept.com/2015/01/26/secret-badass-spy-program/ (accessed 8 July 2016).

[21] C Paton, "Grindr urges LGBT community to hide their identities as Egypt persecutes nation's gay community" available at http://www.independent.co.uk/news/world/africa/grindr-urges-lgbt-community-to-hide-their-identities-as-egypt-persecutes-nations-gay-community-9757652.html (accessed 8 July 2016). Note that in most jurisdictions warrants are required for remote access to computing systems.

[22] Joseph Turow et al, "Americans Reject Tailored Advertising and three Activities that Enable it." (2009) *SSRN 1478214*.

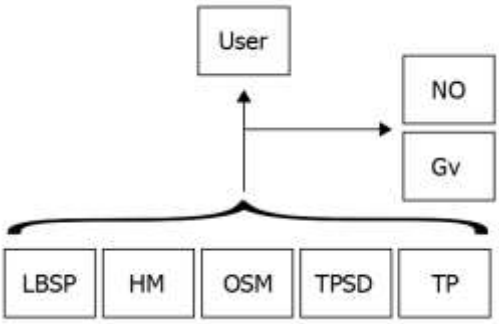

Figure 3: Information flow back to the user in form of personalisation.

4.5 Identifying Principles of Transmission

Although there are many reasons for people to travel, most types of offline travel activities – i.e. travel without using online LBSs – include the following information flows: a company, such as a railway company or hotel, sells tickets or rents accommodation that indicate the traveller's current, past or future location at certain times. Due to space constraints, we elaborate on the transmission principle in relation to the examples of a train company and a hotel but note that our reasoning can be applied to many other scenarios, such as any kind of travel activity that requires a reservation. Activities that require no reservation, like buying museum tickets with cash, may entail fewer or less extensive information flows in an offline scenario.

A leisure trip usually includes booking a means of transportation, booking hotels and telling family or friends about the trip. For the means of transportation, let us consider the example of a train ride. The information exchanged with the train company depends on the way the ticket was purchased. In the most anonymous case, the ticket is purchased at a counter or machine and paid with cash. In this case no information is exchanged but that an unidentified passenger intends to travel a certain route. If, however, a credit card is used, then more information is included in the sale, allowing the train company to link travels booked with the same credit card.[23] Furthermore, the credit card company will record the location of the user along with the purchased product. While the credit card company may have legitimate reasons for collecting this information, such as fraud detection, we note that this practice may not be part of users' legitimate expectations and would justify a CI analysis of its own. Finally, if the purchase was completed using some other account information, such as through a membership in a bonus program or via an online account, the information flow between the traveller and a railway company will include additional details on the traveller such as age, billing address and details of the journey such as time/place of departure/arrival. Regardless of how the booking was completed, the flow of

[23] EU data protection law may prohibit this, but the technology does allow for such linking of different data. Due to the opacity of actual data flows, caused by complexity as well as trade secrets or IP rights, it is difficult to establish which data are actually linked. Precisely for that reason it is pertinent to take into account what is technically feasible. When composing legislation that prohibits such behaviour it seems wise to focus on preventing that such exchanges are feasible (technical and economic disincentives), e.g. by imposing data protection by default coupled with adequate enforcement mechanisms (administrative fines and tort liability). This is precisely what the upcoming GDPR does (art. 23 GDPR imposes a legal obligation to develop data protection by default and design; art. 83.6 determines that fines of up to 4% of global turnover can be imposed by the supervisory authority).

information is governed under several transmission principles: *reciprocity* and *consent* as the information is necessary for the monetary exchange for a service; *necessity*, *accuracy* and *completeness of data* because without the correct information, the railway company is not able to issue the correct train ticket; *purpose binding* because the user has a reasonable expectation that the railway company will only use this information for selling the ticket; and *confidentiality* because the traveller expects to keep records about her journeys private.

The information a traveller needs to reveal to the hotel is governed by the same transmission principles. With respect to the traveller's family and friends, a traveller may inform them with various details about her journey. The involved transmission principles are *reciprocity* since it is common that friends and colleagues inform each other of their travel plans; or *confidentiality* when it is clear that the traveller does not want a friend to pass on information about her travel plans. We note that anyone with information on someone's travel could infer more or less accurate real-time whereabouts of this person. For instance, a person knowing that someone stays in a hotel for a certain period is able to infer that this person is likely to be in the hotel during night. A similar argument can be made based on knowing that someone takes a train at a specific time. In an offline context, however, such inferences are always based on guesses and have a limited accuracy.

We note that – especially in data-driven scenario's - the outlined primary information flows may result in subsequent information flows directed to tax authorities (for fraud detection), justice and police (for criminal investigations) and intelligence services (for the prevention of threats to national security or the gathering of intelligence information). In this section we focus on the primary information flows, generated in a commercial context. We also note that in the subcontexts of work-related travel and immigration extra information flows may occur, as employers or immigration services may either tap into existing information flows or establish their own infrastructure to keep check of the location of their employees or potentially illegal immigrants.

4.6 Locating Applicable Entrenched Informational Norms and Points of Departure

As in the case of our reasoning about transmission principles, we argue that the entrenched informational norms and points of departure are similar for most types of leisure travel, though it should be clear that in the sub-contexts of work-related travel and immigration other informational norms will be at stake. In the following we distinguish between two cases of information collected in offline traveling activities. First, we address the expectations of how a service provider will use the location data. Second, we examine the circumstances under which a company is allowed to share information on the traveller's location with other entities.

A train traveller or hotel guest can expect that the information she provided to the railway or the hotel is in some sense used for an internal review of their business processes. The traveller or hotel guest should not expect an unknown business model based on the monetisation of her location data. For example, every company needs to aggregate basic statistics about its customers, but a railway company sending advertisements to their customers that include detailed information about the travel behaviour of a particular customer would not be in line with entrenched informational norms. A judgment on whether these norms are violated if the customer data is transferred to another organisation depends, amongst others, on the type of organisation. For example, selling customer information to a data broker can be

problematic even if they are pseudonymised, because this implies that data brokers learn about the traveling behaviour of people with whom they never had any business. However, access to customer data based on a legal obligation, such as tax law, may be acceptable to the extent that tax authorities must be capable of inspecting a company's accounting system. Further problems arise if law enforcement, immigration services and intelligence services gain unrestricted or mostly invisible access to these types of data. Several years ago, the Dutch navigator TomTom found its reputation damaged when users found out that their aggregated data were used to predict traffic violations at certain road tracks.[24] Such examples clarify that in a travel context, people do not expect their location data (and what can be inferred from them) to end up with third parties whose access they cannot foresee. Some would claim that even if they would – cynically – expect this, it would still violate their reasonable expectation of privacy concerning this travel data.

4.7 Prima Facie Assessment

The purpose of the prima facie assessment is to determine whether there are red flags attached to changes or violations of entrenched informational norms due to a new socio-technical practice or if an entirely new information flow is being created. It is easy to see that both are the case. LBSs change the described information flows, because they generate, store and mine not merely volunteered data (as was always the case) but also massive flows of behavioural data that were simply non-existent before the massive employment of web services. Buying a train ticket hardly gave the train company any insight on the buyer's location, besides perhaps the location of the purchase. Offering the purchase of tickets via an app, however, may allow the train company to constantly track the user.[25] Entirely new information flows are being generated since numerous companies, such as LBSP, TPSD, OSM, HM and third parties, potentially gain direct access to a traveller's location data whenever she is using LBSs.

4.8 Evaluation I

In the first part of the evaluation, we assess how the new socio-technical practice generates threats to autonomy, potential harms, how it affects the existence of freedom, power structures, justice, fairness, equality, social hierarchy, and democracy.

As we have laid out in Section 2.3 and Section 4.4, various entities may gain access to accurate location data. This may be either because the user herself transmits location data (volunteered data) or because some software, running on the user's MD, is covertly transmitting location data to second or third parties (observed data, whether with or without consent, whether legal or illegal). From a privacy perspective this is highly problematic, because the collection and analysis of accurate location information allows for the inference of highly sensitive information about an

---

[24] A Preuschat and H Luttikhedde, "TomTom to Bar Police Data Use" available at http://www.wsj.com/articles/SB10001424052748703922804576300390277973646 (accessed 8 July 2016).

[25] JP Achara et al, "Detecting Privacy Leaks in the RATP App: How we Proceeded and what we Found" (2014) 10 *Journal of Computer Virology and Hacking Techniques* 229-238.

individual. Users of LBSs may be confronted with these inferences either immediately or in the future, where the 'future' could be minutes, days, weeks and even up to years and decades ahead since location data, once available, may persist in Big Data Space.[26]

The *power structure* and *fairness* in the market is threatened, because the user may be disadvantaged when negotiating with a company that has access to her location data. For example, an LBS user may find herself in a situation where she has to pay a higher health insurance premium or is even rejected for insurance. If an LBSP, or any TPSD whose software is embedded in the LBS, tracks the user's whereabouts it may sell this location data to a data broker specialised in health risk assessment. The analysis of this data broker may be based on the user being relatively more often in health related facilities, which may result in assigning this user a higher health risk. An insurance company that consults the data broker may then decide that it either increases premiums or refuses insurance all together. Note that in this scenario the user would have no idea how the insurance company reached its decision, nor would she be able to correct false predictions[27] about her health. One could think of numerous other examples of how the user would be disadvantaged when negotiating with an entity that knows her whereabouts. The traveller's *autonomy* is at stake, because she is unable to inspect and correct the inferences made in the BDS. This may have severe consequences, including unwarranted or even prohibited discrimination.

There are further implications in recent revelations which have shown that intelligence agencies have a strong interest in location data to enhance their surveillance systems.[28] While one can only speculate on how this data is being used, the very existence of such programs threatens society in several ways. A government with access to location data of a large majority of the population is able to determine which people have contacts with refugees or protesters and could thus effectively prohibit or even pre-empt demonstrations or free speech.[29] These threats to democracy and *justice* are also simultaneously threats to *freedom* and *equality* since authoritarian states may imprison or discriminate people based on their location data (mobility) and the inferences drawn from them. Finally, the US government uses location data to coordinate drone strikes to kill people qualified as enemy combatants without due process and with disastrous results for those standing around (qualified as collateral

---

[26] On the threats that emerge in the combination of location and other types of tracking see e.g. JH Ziegeldorf et al, "Privacy in the Internet of Things: Threats and Challenges" (2014) 7 *Security and Communication Networks* 2728–42.

[27] Inferences made by behavioural advertisers have shown to be wrong: R Ashwini et al, "What do They Know About me? Contents and Concerns of Online Behavioral Profiles" (2015) *arXiv preprint arXiv:1506.01675*.

[28] B Gellman and A Soltani, "NSA Tracking Cellphone Locations Worldwide, Snowden Documents Show" available at http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html and J Ball, "Angry Birds and 'Leaky' Phone Apps Targeted by NSA and GCHQ for User Data" available at http://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data (both accessed 8 July 2016)

[29] On the use of location data by government agencies see e.g. SJ Nouwt et al "Power and Privacy: the Use of LBS in Dutch Public Administration" in B Van Loenen, JWJ Besemer and JA Zevenberger (eds) *SDI Converngence. Research, Emerging Trends, and Critical Assessment* (Optima Rotterdam; Graphic Communication 2009) 75–87.

damage). Though this concerns issues of extraterritorial jurisdiction and international relations, which fall outside the scope of this article, we note that it has a major impact on attempts to establish democracy and the rule of law at the global level.

4.9 Evaluation II

In the second part of the evaluation, we elaborate on how the socio-technical practice of LBS directly impinge on the values, goals, and ends of the context of travel. This particular context is highly relevant for the freedom of movement, and for the fundamental right to be left alone, which entails that by default, it is no one's business where a person travels. However, the usage of MDs and LBSs enables the collection of accurate location data that provides evidence on where a traveller went, for how long and how often. Therefore, the freedom and anonymity of traveling no longer exists as they did, because unforeseeable commercial enterprises as well as governmental agencies may gain access to this information, aggregate it and make it machine searchable. Furthermore, whereas our journeys usually had no impact on other contexts of our life such as business or healthcare, due to the business model of LBSs and increasing governmental surveillance activities, inferences made from location data may reach parties outside the context of travel, with unforeseeable consequences in other contexts, such as employment, insurance and law enforcement.

4.10 Conclusion

Our evaluation shows that the new socio-technical practice of LBSs comes with significant threats for their users. Organisations may gain access to accurate location information, which enables them to infer sensitive information. These inferences may be used for unknown purposes, and transferred or sold by other, unforeseeable organisations. This may lead to an individual being disadvantaged due to the knowledge these organisations have about her. Even worse, people have no practical means to realise or escape this situation since the collection, transfer and processing of their location data is entirely opaque. Furthermore, individuals are mostly *unaware of and unable to correct* false inferences, as well as *unable to object to* unfair targeting. Finally, as we have argued, the new socio-technical practice introduces threats not only to individuals, but also to society at large.

We acknowledge that LBSs are undoubtedly useful and may enhance our daily lives. Solutions like PocketFinder may help to prevent harm and danger to children and elderly. Location data may serve to identify credit card fraud or to find stolen vehicles. If the collection of location data happens in a transparent way with obvious ways for an individual to opt-out and to control inferences being made from her location data, we would accept that the new informational norms may be beneficial and should be embraced. However, the hidden collection of location data by numerous entities capable of using this data in unforeseeable ways is not justifiable and clearly violates the integrity of the context of leisure travel. As this implies a violation of the reasonable expectation that people have concerning their privacy, this should be considered an unjustified breach of privacy.

5. The Complexities of Intertwined Contexts

LBSs are ubiquitous in their nature and becoming increasingly omnipresent. As we have seen above, a crucial step in Nissenbaum's decision heuristic is defining the

prevailing context. This raises the question of what counts as a context and how one can identify the prevailing context. A context can be seen as an overarching social institution, an architecture that attributes roles and mutual expectations, which guide the interactions between people. Institutions – in the sociological sense of the term – determine how behaviours are "read" and which actions are deemed appropriate. A context in this sense entails the institutional environment that hosts more specific institutions, such as for instance marriage, church, school or corporate enterprise, that are part of, respectively, the contexts of family life, religion, education or economics. Depending on the context, different informational norms and transmission principles will apply and prescribe the appropriateness of the information flows. As indicated in the previous section, this entails that the choice of the prevailing context is both the gateway and the vanishing point of the CI decision heuristic.[30]

The assessment of contextual integrity and its violation becomes complex when the assessor has to deal with two or more (sub)contexts. Multi-layered and overlapping contexts make it rather difficult to pinpoint only one "right" context as the prevailing one. Not only will a service rendered to the subject trigger sharing of location data, but, as we have seen above, location data is shared on many levels simultaneously and subsequently. Such sharing may involve various contexts, for instance, a commercial context (behavioural advertising based on shared location data captured by the LBS), a health context (LBS activated when traveling to a hospital) or a work-related context (LBS activated when commuting or travelling for one's professional occupation). This renders the analysis of an isolated information flow inadequate as a criterion to decide on the prevailing context. Therefore, we have opted for the travel context, which is at stake in each of the scenarios where LBSs are employed.

Even so, one could argue that in each of the scenarios the overarching context is that of economics, which would imply competing prevailing contexts. With an eye to advancing "the state of privacy", Nissenbaum has revisited her theory to defend it against misconceptions by policy makers. Recalling her definition of context as a social domain or social sphere that provides organising principles for legitimate privacy expectations, she differentiates her understanding of context from three others. First, from context as a technology system or platform; second, from context as a business model or business practice; and third, from context as sector or industry.[31] We are not sure that this resolves the problem of competing prevailing contexts, since commerce is itself a social domain that penetrates many other social domains. The problem may be that social domains are (no longer) mutually exclusive. Since choosing a different prevailing context might lead to a completely different outcome, as entrenched transmission principles and informational norms will differ, we need to face the pivotal question of who gets to decide on the choice of the prevailing context: the service provider, the data subject, the people, the social scientist, the ethicist? Who is the assessor?

If we take into account that different contexts lead to different results, qualifying a context as prevailing has far-reaching implications. One could therefore conclude that

---

[30] In that sense, context seems to be given rather than the result of struggles and reconfigurations. See the praise and the critique of R Bellanova "Waiting for the Barbarians or Shaping New Societies? A Review of Helen Nissenbaum's *Privacy in Context* (Stanford: Stanford University Press, 2010)" (2011) 16 *Information Polity* 391-395, notably at 394.

[31] H Nissenbaum (2015), see note 2 above.

the choice of context is not only the gateway to the CI decision heuristic, but also its vanishing point. Once the heuristic has progressed beyond the second step, potentially conflicting norms and principles that pertain to other contexts have become invisible. In our case, to come to a sustainable conclusion as to violations of CI in the case of LBSs, we would need to develop the decision-heuristic for a number of relevant contexts, such as e.g. economics, travel, health and education, depending on the situation or scenario. This could lead to conflicting transmission principles and informational norms and would basically require deciding which context should be qualified as the primary or overruling context amongst several prevailing contexts. It is not obvious that this decision can be made at a general level for each instance where LBSs are employed. If that means that we must decide per situation which context is primary, the heuristic no longer provides clear guidelines to evaluate the impact of LBS on contextual integrity. We believe, however, that this rather tricky challenge is not something we should resolve. On the contrary, it sensitises us to the fact that location is no longer equivalent with context, as it perhaps used to be (with separate spaces for work, family life, religious worship and leisure time). It also means that the principle of purpose limitation may be a more apt criterion to decide on the legitimacy of an information flow (as well as other types of processing), taking into account the context(s) on a case-by-case basis.

6. Contextual Integrity and Purpose Limitation

6.1 The Legal Obligation of Purpose Limitation (PL)

Contextual integrity and the legal obligation of purpose limitation (PL) share some common ground. Both require for the flow and distribution of personal data to be appropriate, assuming that both collecting and further processing of personal data should be limited. Both look beyond collection, though PL regards any form of personal data processing (including analysis) while contextual integrity seems to be restricted to transmission of personal data. Also, the CI decision heuristic concerns an ethical inquiry, whereas PL is a legal obligation within the jurisdiction of the European Union (EU). Before analysing the CI decision heuristic from the legal perspective, we will first explain the background and content of the legal obligation of PL.

The legal obligation of purpose limitation derives from the OECD Fair Information Principles, as formulated in 1980.[32] Within the context of EU data protection law, it seems to be one of the most crucial characteristics of the protection of personal data (as specified in art. 8 of the Charter of Fundamental Rights of the EU, which defines the fundamental right to data protection). We will now discuss five points to be made for a proper understanding of PL within the legal framework of the EU.

First of all, the 1995 EU Data Protection Directive (DPD), as well as the upcoming GDPR,[33] require that processing of personal data is based on a specific and legitimate

---

[32] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 23 September 1980, updated in 2013, available at http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (accessed 14 Aug 16).

[33] See note 7 above.

purpose made explicit by the data controller. The data controller is defined as the entity that decides the purposes and the means of personal data processing, and is held liable for compliance with the DPD (art. 6).[34] "Purpose" thus serves, first, to define who is responsible for personal data processing, while also, second, providing the person whose data are processed (the data subject) with a clear idea of what they can be used for. Purpose thus determines the relationship between sender and receiver of the data, and includes the case of behavioural data, where the receiver can be seen as actually sending the data to itself. PL, then, seals the relationship between data subject and data controller, and forces the controller to somehow make sure that the data subject "knows" how her data may be used. Depending on the circumstances, the purpose can for instance be specified in a statute (e.g. if the tax administration requires LBS data to determine fraud), or be announced in the terms and conditions of a web service (e.g. specifying that location data will be used for marketing purposes). In the latter case, we may doubt whether the users of the service are aware of the purpose, considering the lengthy privacy policies that hide such information. Especially if the legal ground for the processing concerns "the legitimate interest of the data controller" (as in the case of Google's search engine), the legitimacy of the processing will have to be evaluated on a case-by-case basis to check to what extent the rights and interests of the data subject are being respected.[35]

Second, art. 6.1(a) of the upcoming GDPR states that processing is allowed if "the data subject has given consent to the processing of his or her personal data for one or more specific purposes." In the case of LBSs, this requirement is often sidestepped by demanding consent for the re-use of the location data for the purpose of marketing or monetisation (though the latter is hardly ever made explicit). If such additional consent is refused, the service provider usually simply refuses to contract. Art. 7.4 of the GDPR, however, stipulates that "[w]hen assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract." This would basically mean that PL cannot be eroded by forcing consent for secondary purposes on those who wish to access an LBS. When this stipulation comes into force (in May 2018), LBSs may have to change their business model by, for instance, charging a fee instead of relying upon the monetisation of location data.

Third, the current DPD requires that data controllers do not process personal data for purposes that are incompatible with the purpose they have explicitly specified when initiating the processing of the data (at the time of first collection). Though it seems

---

[34] Art. 6 DPD (and art. 5 GDPR) stipulates purpose limitation and holds the data controller liable. Art. 2(d) DPD (and art. 4.7 GDPR) specifies that the data controller is the entity that determines the purpose and means of the processing of personal data.

[35] This relates to the so-called f-ground for legitimate processing of personal data (art. 7.f DPD, art. 6.1.f GDPR), which allows for processing on the ground of necessity "for the purposes of the legitimate interests pursued by the controller of by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection (…)." In CJEU 13th May 214, C-131/12 (*Google Spain v Costeja González*), the European Court of Justice of the EU decided that Google Spain processes the personal data of those listed in the search results on the basis of the legal ground of art. 7.f and found that the economic interest of the search engine provider can – in general – not overrule the fundamental rights of the data subject.

that the OECD Guidelines allowed for a person to give consent to process her data for other or even any purposes,[36] the DPD clearly stipulates that purpose binding holds, even in the case of consent.[37] This means that even under current law, consent to process one's data for whatever purpose is not valid. It also entails that reuse of personal data for incompatible purposes is only lawful after the data have been fully anonymised, or after informed and freely given consent has been obtained for the new purpose (taking into account art. 7.4 as discussed above).[38] Together with the proportionality principle, European law thus prevents excessive processing of personal data. The proportionality principle refers to art. 9 DPD and stipulates that the processing of personal data needs to be adequate, relevant, and not excessive in relation to its purpose.

Fourth, to the extent that data processing infringes the privacy of a person, the proportionality principle also relates to the issue of whether such processing is proportional, considering the legitimate aim it serves. This links the DPD with art. 8 of the European Convention of Human Rights (ECHR) that enshrines the right to privacy. Art. 8 determines that whenever a measure infringes the privacy of a person, the measure that constitutes the interference must be justified on the basis of a triple test. First, the infringement must be directed to a legitimate aim. Such aims are limitatively summed up in art. 8.2, but formulated in such a broad manner that this is seldom a problem. Second, the infringement must be "in accordance with the law", meaning that the infringement is based on a legal norm that is accessible and foreseeable while incorporating the necessary safeguards for the person whose privacy is infringed. Relevant safeguards may regard the limitation of the scope and the duration of the infringement, a right to object and the need to obtain a warrant or permission from an independent authority.[39] Third, the infringement must be necessary in a democratic society, which implies – according to the case law of the European Court of Human Rights – that there is a pressing social need for the infringing measure.[40] This – third – part of the triple test, is interpreted in terms of proportionality; the infringement must be proportional to the aim served, meaning that the measure is appropriate to achieve the aim and not excessive in relation to the aim. The proportionality principle of art. 8.2 of the ECHR regards the processing of personal data only insofar as it infringes one's privacy. Though processing credit card data for the sale of LBSs falls within the scope of the DPD, it is not an infringement

---

[36] Art. 9 of the OECD Guidelines formulates the purpose specification principle; art. 10 the use limitation principle. According to art. 10, however, data can be used for other purposes "with the consent of the data subject or by authority of law". This can be read as meaning that one can consent to waive one's right to use limitation.

[37] EU law requires that processing of personal data is based on one of six legal grounds that legitimate the processing of personal data (art. 7 DPD, art. 6 GDPR); consent is one of these legal grounds. On top of this requirement, the purpose must be explicitly specified and processing must be restricted to the specified purpose or one that is compatible (art. 6 DPD, art. 5 GDPR). This requirement cannot be waived.

[38] See, however, Art. 29 WP Opinion 5/2014, WP216 on anonymisation techniqes, that seems to pratically rule out effective full anonymisation. This entails that such "anonymisation" must be qualified as pseudonymisation from the perspective of the law.

[39] Cf. e.g. ECtHR, 29 June 2006, *Weber and Saravia v Germany*, Appl. Nr. 54934/00, which sums up the safeguards relevant for a measure being qualified as "in accordance with the law", § 95.

[40] Cf. e.g. ECtHR, 26 April 1979, *The Sunday Times v UK* (Series A no 30), § 62.

of one's privacy. The processing of location data by the provider of an LBS may, however, constitute an infringement if it violates a person's reasonable expectation of privacy, notably when data are shared with third parties that link the data with other information to gain a more complete insight into a person's social network or life style. If that third party is a government agency art. 8 will definitely apply. Since the ECHR provides a person within the jurisdiction of the Council of Europe with rights against their governments, it is not obvious that art. 8 always applies to the processing of personal data by other third parties. The so-called direct and indirect horizontal effect of art. 8 may extend the protection to privacy infringements by private parties. Direct horizontal effect refers to e.g. tort law, that could render an LBSP liable for harm caused if it infringes the privacy of its customers (e.g. by sharing location data with parties capable of building invasive profiles with additional data).[41] Indirect horizontal effect refers to a positive obligation of the state to protect its citizens against privacy infringements by private parties. Considering the fact that the fundamental right to data protection explicitly requires Member States of the EU to implement this right in relation to non-state actors, such positive obligations may indeed give rise to liability of the state on the nexus of privacy and data protection.[42]

To determine the meaning of a legal text that has force of law, such as the DPD or the upcoming GDPR, lawyers will usually refer to relevant case law, which also has "force of law". Based on art. 29 of the DPD, however, a Working Party was established to advise on the interpretation of the DPD. Though its interpretation is not legally binding, it has considerable authority and its Opinions must be considered when deciding the meaning of the DPD. In 2013, the Art. 29 Working Party issued an Opinion to clarify the meaning of the principle of purpose limitation that further elucidates how this legal obligation operates and how data controllers should implement purpose binding in their personal data life cycle management.[43] The Working Party notably concerns itself with the interpretation of what constitutes a compatible or incompatible purpose, since this determines when processing is no longer lawful.[44] A change of purpose will usually be relevant when personal data are reused or recycled in relation to other business models or by third parties that may provide entirely different services that cannot be understood as serving a compatible purpose. For instance, if an LBS stores location data for longer than strictly necessary to fulfil the contract (to provide friends with one's location, to offer promotions of nearby shops, to calculate the invoice), the LBS needs to check whether this is still

---

[41] Cf. e.g. E Frantziou, "The Horizontal Effect of the Charter of Fundamental Rights of the EU: Rediscovering the Reasons for Horizontality" (2015) 21 *European Law Journal* 657-679, at 666. Frantziou distinguishes between direct and indirect horizontal effect and positive obligations. For the sake of space constraints, we will not enter this discussion, but we note her argument (at 672-3) that horizontal effect also relates to the fact that fundamental rights are not merely individual interests but also collective goods.

[42] Also, art. 82.1 GDPR requires that "Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered." Art. 82.2 states that "Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller."

[43] Art. 29 WP, Opinion 03/2014, WP 203 on purpose limitation.

[44] *Ibid*, at 20-36.

compatible with the specified purpose it explicitly expressed when first processing the data. The Opinion clarifies that compatibility as to the original purpose must be decided on a case to case basis, taking into account the following key factors:[45]

1. The relationships between the purposes for which the personal data have been collected and the purposes of further processing;
2. The context in which the personal data have been collected and the reasonable expectations of the data subjects as to their further use;
3. The nature of the personal data and the impact of the further processing on the data subjects;
4. The safeguards adopted by the controller to ensure fair processing and to prevent any undue impact on the data subjects.

As to the further use of location data, this entails, first, that reuse for an entirely unrelated purpose (e.g. tax fraud detection) is problematic. Second, it implies that the fact that sensitive data may be inferred from location data indicates the need to be cautious about concluding that a purpose is compatible, notably when such data or their inferences can have adverse effects on a data subject (rejection for an insurance or a job interview, detailed monitoring by law enforcement agencies based on risk assessments that rely in part on location data, paying a higher price for consumer goods due to having visited shops on the high end of the market). Third, much will depend on the question of whether adequate safeguards have been implemented, for instance, pseudonymisation of energy usage data that include location data. Interestingly, the Working Party finds that the context in which the data have been collected is a key factor to determine the compatibility of the purpose. This links with the idea of contextual integrity, though we note that context is only one of the key factors, rather than the sole criterion to decide the legitimacy of personal data processing.

6.2 Interfacing CI and PL

Some authors believe that the PL obligation is a consecration of Nissenbaum's CI theory.[46] Others believe that the CI theory is not very relevant for non-US jurisdictions that have a framework of general data protection law that incorporates PL.[47] As a point of departure we note that, though her theory may be used to add clarity to the legal framework, CI covers only the flow of information and depends entirely on the original context of disclosure.

As such, *firstly*, the scope of PL within the legal framework is broader than merely the transmission and distribution of personal data within an identifiable context, as it includes any processing operations performed on personal data that are stored (where

---

[45] *Ibid*, at 23-27.

[46] F Dumortier, "Facebook and Risks of 'De-contextualization' of Information" in S Gutwirth, Y Poullet and P De Hart (eds) *Data Protection In a Profiled World* (Dordrecht: Springer, 2010) 119-137.

[47] CJ Bennet, "Book Review: Nissenbaum, Helen (2010) Privacy in Context: Policy and the Integrity of Social Life. Stanford: Stanford University Press" (2011) 8 *Surveillance and Society* 541-543, at 542-543.

no data flow is at stake). We note that EU data protection law holds specific protection for location data, even if it cannot be qualified as personal data.[48]

Second, the scope of PL is broader in that it considers the processing of personal data in other contexts without assuming that such processing is necessarily illegitimate whenever it takes place in another context. PL depends on the declared intent of – and the usage by - the data controller, taking into account the context of collection.

Third, the scope of protection generated by PL may be eroded if data controllers specify a broad purpose or a whole range of purposes when they collect the data. In that case, PL may provide little protection other than forcing data controllers to determine and make explicit the relevant purposes before they start processing. The requirement of specificity should actually prevent overly broad purpose determinations, but so far both private and public entities often resort to either very broad formulations of purposes (e.g. "to improve the provision of services"), or to whole series of specific purposes (e.g. to detect tax fraud and social security fraud, or to achieve compliance with the principle of 'collect only once' in the context of e-government). As a matter of fact, the lack the protection caused by broad definitions or multiple disparate purposes is due a lack of enforcement; if data protection authorities were to have the competence to impose adequate fines, the requirement of explicit specification should be sufficient to prevent erosion of the obligation. A similar lack of the protection is inherent in the notion of context. Notably, policy makers, courts or data controllers may decide that in the case of LBSs the prevailing context is commercial, whatever other context is at stake. The same goes for the prevailing context of national and public security, which often overrules any context, even the commercial one. The lack of the protection offered by CI due to either the overruling context of commerce or that of public security is inherent in the difficulty of identifying the prevailing context, especially when more than one prevailing context is at stake, depending on one's perspective.

Fourth, PL is a legal obligation that creates civil and administrative liability for data controllers, whereas CI is an ethical theory that invites citizens, policy makers and business undertakings to consider what should count as appropriate data flows and appropriate distribution of personal data. Though a law that does not even aim to achieve justice cannot be qualified as law in a constitutional democracy, law is both more and less than ethics. Law also aims for legal certainty and purposefulness.[49] This implies that its scope is both more restricted than ethics (for instance, if achieving justice is at odds with legal certainty, notably where people disagree about what is just in a particular context) and broader (for instance, where no agreement can be found on what constitutes an appropriate and properly distributed information flow, the law will provide for legal certainty and decide on such issues in line with PL and proportionality).

---

[48] See notably art. 9 ePrivacy Directive 2002/58/EC, concerning the processing of personal data and the protection of privacy in the electronic communications sector. On the intricacies concerning the legal regime for location data, see C Cuijpers and BJ Koops, "How Fragmentation in European Law Undermines Consumer Protection: the Case of Location-Based Services" (2008) 33 *European Law Review* 880–897.

[49] M Hildebrandt, "Radbruch's Rechtsstaat and Schmitt's Legal Order: Legalism, Legality, and the Institution of Law" (2015) *Critical Analysis of Law* 2, available at http://cal.library.utoronto.ca/index.php/cal/article/view/22514 (accessed 16 Aug 16).

Taking account of these differences, we shall now see how context fits into the decision on the lawfulness of reuse of personal data, by referring to the second key factor for determining whether its purpose is compatible with the initial, explicitly specified purpose. As discussed above, this key factor concerns "the context in which the personal data have been collected and the reasonable expectations of the data subjects as to their further use." Indeed, this implies two things. First, it implies that processing personal data should be aligned with the reasonable expectations that come with the context where they were first collected. This points to the relevant transmission principles and informational norms of the CI heuristic. Second, it implies that processing such data in another context is not prohibited, but that to determine the legitimacy of cross-contextual processing, the expectations raised in the original context are critical. In a sense, this key factor seems to integrate the CI heuristic into the determination of the compatibility of the purpose. At the same time, it does not make the CI heuristic decisive as other key factors must be taken into consideration. As a consequence, the original context does not over-determine the judgement on whether or not the processing of location data is legitimate, though it plays a key role.

In art. 35 of the upcoming GDPR, a new legal obligation is established that requires data controllers that wish to employ new technologies to assess whether these technologies generate high risks for rights and freedom of individuals. If this is the case, the controller should perform a data protection impact assessment (DPIA).[50] We note that the CI decision heuristic provides an interesting framework for such an assessment, while the DPIA has the added advantage of requiring an assessment of mitigating measures,[51] thus integrating the notion of data protection by design and default into the assessment.[52] It is pivotal that users of LBS have access to ways and means to protect themselves against persistent tracking and tracing.[53] However, by imposing DPbD, the GDPR obliges providers to develop architectures *on their side* that protect location privacy, which seems crucial to incentivise the market for DPbD.[54] We therefore believe that the CI heuristic and the DPIA should inspire and test each other, notably with respect to the assessment of the risks to the rights and freedoms of individuals. This would enable a more stringent assessment of how PL and CI contribute to reducing such risks, while providing users with a better grasp of

---

[50] Art. 35.1 GDPR: "Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks."

[51] Art. 35.7.d GDPR.

[52] In art. 25 GDPR, a new legal obligation requires "data protection by default and by design." See M Hildebrandt and L Tielemans, "Data Protection by Design and Technology Neutral Law" (2013) 29 *Computer Law & Security Review* 509–521.

[53] See e.g. F Brunton and H Nissenbaum, *Obfuscation: A User's Guide for Privacy and Protest* (Cambridge, MA: MIT Press, 2015). M Herrmann et al, "Optimal Sporadic Location Privacy Preserving Systems in Presence of Bandwidth Constraints" (2013) *12th ACM Workshop on Workshop on Privacy in the Electronic Society* 167-178, available at https://securewww.esat.kuleuven.be/cosic/publications/article-2376.pdf (accessed 22 Aug 16).

[54] See e.g. M Herrmann et al, "Practical Privacy-Preserving Location-Sharing Based Services with Aggregate Statistics" (2014) *Proceedings of the 2014 ACM Conference on Security and Privacy in Wireless & Mobile Networks* 87-98, available at https://securewww.esat.kuleuven.be/cosic/publications/article-2423.pdf (accessed 22 Aug 16).

how they may be targeted based on the location data they leak. On top of that, the force of law that "backs" PL, in combination with legal obligations to conduct a DPIA and to implement DPbD, should create a market for socio-technical design solutions that support PL.

7. Conclusion

In this work, we investigated the privacy implications for users engaging in LBSs and the sharing of their location data with remote services. We used Nissenbaum's CI heuristic as a framework to perform the assessment in a structured way. We applied CI to our case and we modeled all involved parties that may get access to location data and further modeled the relevant information flows. This revealed that users rarely share their location data with only the LBSP but end up sharing the data with a series of other entities, such as TPSD, OSM, HM or the Gv.

The context in which a user revealed her location is key in Nissenbaum's heuristic when evaluating whether the user's privacy has been breached. Unfortunately, LBSs are used in such a ubiquitous manner that it is impossible to conduct the CI heuristic for every possible context in which users may find themselves when engaging with LBSs. This is not a drawback of the CI heuristic, but inherent in the use of mobile devices that result in the integration and overlapping of different contexts at the same time and the same place. In the case of LBSs, we found that the prevailing context is that of travel, though one can argue that it will often coincide with the prevailing contexts of commerce and public security. Focusing on the context of travel, we show that LBSs create new information flows and alter existing ones with the result that numerous parties obtain users' accurate location, resulting in threats to the user's fair treatment, her autonomy, and other fundamental rights and freedoms. This is because location data exposed via mobile applications may be recorded by LBSs for an unlimited period of time and can be exchanged with a wide variety of parties (even though this would be unlawful under EU law). A user's location data may thus be combined with lifelong movement profiles, which are machine searchable and could be used in many unforeseeable ways to draw inferences about the individual, even far into the future. This in particular is an issue since the user has few effective means to access, let alone control, the information flows that instigate personalised targeting. To assess the extent to which control is lost, and whether this violates reasonable expectations of privacy, we considered the concept of contextual integrity in relation to the principle of purpose limitation.

From a legal perspective, the processing of personal data within the scope of the DPD (and the upcoming GDPR) requires a legitimate, specific and explicit purpose, which restricts the proliferation of location data and the inferences it affords. Currently, however, the requirements of legitimacy, specificity and explicitness are often circumvented by LBSP by formulating very broad terms of use hidden in lengthy terms of service or privacy policies, or by trading free services for extensive invisible profiling. We hope and expect that the upcoming GDPR will enable a more effective enforcement that makes potential usage of location data foreseeable and enables data subjects to object to the processing of excessive or irrelevant data. In its Opinion on purpose limitation the Art. 29 Working Party has clarified that the context is key when assessing whether the purpose of processing is compatible with the original purpose. This context argument nicely links PL to Nissenbaum's CI heuristic and we elaborate on the differences and similarities of the two: Firstly, PL is a broader

concept because CI determines privacy violations only if data is being *transmitted*, whereas PL concerns all types of processing, including analytics. PL is also broader because a violation of PL does not necessarily depend on the context; processing the data in the same context for another purpose may be a violation of PL, where it may be acceptable in terms of CI (depending on whether it violates an informational norm of that context). Secondly, whereas PL may be circumvented by entities stating very general purposes or a long series of specific purposes allowing for almost any processing, CI may be circumvented by defining the prevailing context in a way that enables it to overrule informational norms and transmission principles of overlapping prevailing contexts, notably those of commerce and public security. In that sense much depends on enforcement in the case of PL and the perspective taken by the assessor in the case of CI. Thirdly, CI is an ethical theory that offers a structured approach to reflect on and assess privacy as contextual integrity, whereas PL is a legal obligation, that has legal effect such as liability and the right to object.

Context is everything, but not everything is context. Purpose limitation enables both foreseeability and holding LBSP to account in a court of law, if the law is enforced. We conclude that both concepts are pivotal for a sustainable and responsible employment of location data, noting that the CI decision heuristic should inform the templates of the Data Protection Impact Assessment that will soon be a legal obligation within EU jurisdiction.