International Journal of Geo-Information

MDPI

Article

Location Privacy in the Wake of the GDPR

Yola Georgiadou *,†,‡, **Rolf A. de By** ‡ **and Ourania Kounadi** ‡

Faculty of Geo-information Science and Earth Observation (ITC), University of Twente, 7522 NB Enschede, The Netherlands; p.y.georgiadou@utwente.nl (Y.G.); r.a.deby@utwente.nl (R.A.d.B.); o.kounadi@utwente.nl (O.K.)

* Correspondence: p.y.georgiadou@utwente.nl

† Current address: University of Twente, Faculty ITC, PO Box 217, 7500 AE Enschede, The Netherlands

‡ These authors contributed equally to this work.

Received: 13 February 2019; Accepted: 15 March 2019; Published: 22 March 2019

Abstract: The General Data Protection Regulation (GDPR) protects the personal data of natural persons and at the same time allows the free movement of such data within the European Union (EU). Hailed as majestic by admirers and dismissed as protectionist by critics, the Regulation is expected to have a profound impact around the world, including in the African Union (AU). For European–African consortia conducting research that may affect the privacy of African citizens, the question is '*how to protect personal data of data subjects while at the same time ensuring a just distribution of the benefits of a global digital ecosystem?*' We use location privacy as a point of departure, because information about an individual's location is different from other kinds of personally identifiable information. We analyse privacy at two levels, individual and cultural. Our perspective is interdisciplinary: we draw from computer science to describe three scenarios of transformation of volunteered or observed information to inferred information about a natural person and from cultural theory to distinguish four privacy cultures emerging within the EU in the wake of GDPR. We highlight recent data protection legislation in the AU and discuss factors that may accelerate or inhibit the alignment of data protection legislation in the AU with the GDPR.

Keywords: location privacy; GDPR; European Union; inference; privacy cultures; African Union

1. Introduction

On 25 May 2018, two years after its enactment into law, the General Data Protection Regulation (GDPR), "*the most contested law in the E.U.'s history, the product of years of intense negotiation and thousands of proposed amendments,*" became enforceable in the European Union [1]. The GDPR protects the processing of personal data of natural persons and allows the free movement of such data within the European Union (EU). Unlike the Data Protection Directive (DPD) of 1995, which GDPR repealed, 'Regulations' are directly applicable as statutory law across the Union, and are not amenable to the opportunistic transposition of 'Directives' within individual Member States. A blatant example of a Member State transposing the DPD of 1995 and at the same time courting non-EU tech companies with weak enforcement and advantageous tax schemes was the Republic of Ireland [2]. Ireland's transposition allowed tech companies to develop an EU site with such favorable conditions that Facebook shifted its headquarters for all of its global business outside North America to Ireland. Only in late April 2018, just before the GDPR took effect, did Facebook move more than 1.5 billion users out of Ireland and out of reach of the new law, despite Mark Zuckerberg's promise to apply the spirit of the GDPR globally [3].

International flows of personal data are becoming more significant than ever. The EU trades with the US some $260 billion worth of digital services annually, much of which involves personal data [4]. Data flows increased the global GDP, of which an estimated $2.8 trillion represents data

flows, by $7.8 trillion in 2014 [5]. These economic facts coupled with the data protection asymmetry between countries explain much of the global interest in the GDPR, ever since its enactment in 2016. International commentators' views of the GDPR are oscillating between ecstatic and dismissive. Daniel Solove, a leading American scholar of privacy law, lauded the GDPR as the "*most profound privacy law of our generation*," "*majestic in its scope and ambition*." He even professed his love for the GDPR, because of the law's broad definition of personal data and its attention-grabbing penalties, among other things [6]. Other non-EU analysts consider GDPR the "*most consequential regulatory development in information policy in a generation*" [2], "*a new paradigm in data privacy*" [7], "*a real chance to renegotiate the terms of engagement between people, their data, and the companies*" [8], and the thing that will bring surveillance capitalism [9] to its knees [10]. On the other hand, American critics dismiss GDPR as 'EU protectionism' and for its ability to achieve important European geopolitical goals including "*(1) solidifying legitimacy for Brussels during a period of deep skepticism among voters, and (2) strengthening European political power against the real or perceived threat of American digital prowess*" ([11], page 236). Most importantly, they are unconvinced by the EU's independent data protection authority billing itself the "*global gold standard*" [12] in data protection and call attention to the substantial historical and cultural differences across nations that may inhibit exporting the GDPR as a one-size-fits-all approach to other countries.

The latter critique is warranted. Like all human societies, the EU and the US have different and deeply entrenched cultures of privacy. European privacy law protects human *dignity*, a right rooted in the devastating experience with Fascism and Nazism, and in the ruling of the German Federal Constitutional Court in its celebrated Census case of 1983 for informational self-determination [13]. In the EU, the constitutional protection of dignity is anchored in Article 8(1) "*Everyone has the right to the protection of personal data concerning him or her*" of the Charter of fundamental rights of the European Union (2000/C 364/01). Privacy law in the US protects *freedom*, especially freedom from intrusions by the state—not by private corporations—in the sanctity of one's own home [14]. The word privacy is not mentioned in the US Constitution, except indirectly in the Fourth Amendment, which prohibits the violation of "*the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures*." One of the most significant constitutional safeguards for information in the US concerns the free flow of data in the First Amendment's free speech clause. Thus EU privacy legislation engages in a rights-based discourse centered on the dignity of the 'data subject'—the individual citizen whose data is processed and whose information is at stake. The US situates the individual squarely in marketplace relations trading her personal information in free exchanges as a 'consumer,' exercising a free speech of sorts [4]. These fundamental differences in privacy cultures between two ostensibly similar western polities suggest how difficult it may be for the rest of the world to free ride on Europe's GDPR rules as the enthusiasts claim [15]. The differences also suggest that a more complete account of privacy warrants tracking it at two levels, individual and cultural [16,17]. To distinguish democratic from authoritarian societies, Westin [18]—probably the most influential privacy scholar of the last century—also examines a third, political level of privacy, which is beyond the scope of this study.

In this paper, we distinguish two levels of privacy—individual and cultural. We focus on information privacy, and in particular on location privacy, or geoprivacy. The term location privacy suggests that while control of location information is the central issue, location can be inferred from people's interests, activities, and socio-demographics, and not only from 'traditional' location information, e.g., geographic coordinates [19]. Focusing on location privacy, argue Keßler and McKenzie, is necessary because "*information about an individual's location is substantially different from other kinds of personally identifiable information*" ([19], page 5), for several reasons including: the ease of capturing an individual's location, the improvement of a service when the user shares her location with a service provider, as well as the potential for inferring sensitive information about her social, economic or political behavior from her location history. We define (location) privacy as the positive right to control the collection, access, recording, and usage of an individual's (location) information and determine when, how, and to what extent it is processed by others [20]. We distinguish between privacy

as a negative right (freedom from interference) and privacy as a positive right (freedom to control). Freedom as a negative right, or '*the right to be left alone*' [21], is a notion first used by Warren and Brandeis in their groundbreaking law review essay in 1890. In this essay, written in pre-digital times, they argued for the right of individuals to be sheltered from intrusive photographers of newspaper tabloids of the time. New, digital technologies can now reduce the private space of individuals but also empower them to use the very same tools to enhance their freedom to control their privacy [20], but often in combination with social, organizational, or legal measures or strategies [22]. In the following sections, we first take the point of view of Alice, an individual 'data subject' or 'consumer.' We show how Alice can control (part of) the transformation process of volunteered or observed to inferred information and safeguard her own as well as the privacy of her research subjects from attackers. We then discuss privacy at the cultural level, starting from the basic premise that Alice's (privacy) preferences and commitments are shaped by and shape the culture of her community and society. Privacy preferences oscillate between two extremes:

> "*A high-privacy position assigns primary value to privacy claims, has high organizational distrust, and advocates comprehensive privacy interventions through legal rules and enforcement. A limited-privacy position views privacy claims as usually less worthy than business efficiency and societal-protection interests, is generally trustful of organizations, and opposes most new regulatory interventions as unnecessary and costly*" ([16], p. 434).

We contribute to (location) privacy scholarship in two ways. We complement recent studies (e.g., [19,23,24]) by analyzing (location) privacy at two levels—individual and cultural. We also take a genuine interdisciplinary perspective. We draw from the field of (geo)computing to describe the transformation of volunteered and observed to inferred information and to suggest privacy-safeguarding measures. We draw from organization studies to dissect privacy into ideal types of social relationships and strategies, and from cultural theory to distinguish ideal types of privacy cultures. In the concluding section, we turn our gaze to (location) privacy in the African Union, a polity where currently ongoing legislative activity for personal data protection is matched by an equally intense activity of data extraction from African-based organizations for expert analysis in advanced economies [25,26]. Such an exploration, however tentative, is important to us, because of our long-term engagement with African academia and government in joint research projects, involving African 'data subjects.'

2. Privacy at the Individual Level

2.1. The Individual Data Subject or Consumer

A privacy typology focused on the individual is both problematic and useful. It is problematic at the most basic level of personal data emission, because an individual careless with her personal data exposes information about herself as well as about others. If an algorithm knows her location at a given time, it may predict the location of her spouse or friend. A child posting something about her heart disease on social media may increase her parents' health insurance premium [27]. It is also problematic at the social level because it is the individual's social environment that influences what is deemed personal (data). If a society considers a given mode of personal behavior—e.g., political opinion, sexual orientation, religious or philosophical beliefs, trade union membership (see Article 9(1) of GDPR)—to be socially legitimate, only then is related data deemed personal [16]. On the other hand, a privacy typology focused on the individual is useful. This is because the individual—as 'data subject' or 'consumer'—is the subject of privacy theory and the bearer of the fundamental rights of dignity or freedom. Privacy is a dynamic, ever-changing relationship, or a 'negotiated relationship' [28], between an individual and her environment. It is present in all human cultures; what is culturally specific are the strategies individuals and groups use to negotiate social interaction [29].

2.2. A Typology of Privacy at the Individual Level

At the heart of the privacy typology is Alice, a fictitious (geo)computing scientist, who adheres to the ACM Code of Ethics and the rules of a GDPR-compliant European university. Alice values (location) privacy as her positive right to control the collection, access, recording, and usage of her (location) information and determine when, how, and to what extent it is processed by others [20]. At its simplest, Alice is related to her social environment in four ways—to another individual, to a group of individuals, to a private corporation and to a government institution—arranged in four cells of relations in Table 1. The incongruity of privacy goals between the related parties can be low or high and furnishes the horizontal dimension of the typology. The vertical dimension refers to Alice's ability to control the transformation process of volunteered or observed personal data to inferred data referring to her or to her research subjects. Her ability is high when she can control the entire transformation process—the behavior of humans (including herself), of digital machines and of outputs. It is low when she can control some or none of these [30,31].

Table 1. A typology of (location) privacy relations.

		Goal Incongruity *Low(er)*	*High(er)*
(Alice's) **Ability to control** human behavior, machine behavior, outputs	*Low(er)*	**Cell (4)** Alice – Government institution **Privacy strategy**: Compliance; lodge complaint to DPA in case of violation of GDPR; anti-surveillance resistance	**Cell (3)** Alice – Private corporation **Privacy strategy:** Control behavior of corporation (via GDPR); lodge complaint to DPA in case of violation of GDPR
	High(er)	**Cell (1)** Alice – Bob **Privacy strategy**: Right and duty of partial display	**Cell (2)** Alice – (Bob – Carol – Dan – etc.) **Privacy strategy**: Geoprivacy by design

Before discussing each cell in detail, we draw attention to two obvious simplifications in Table 1. First, in Cell (3), Alice's interaction with a private corporation, for example, a location-based service (LBS) provider, involves not just the LBS provider but twelve other parties. These are the mobile device, the hardware manufacturer, the operating system, the operating system manufacturer, the mobile application, the mobile application developer, the core application, the third-party software, the third-party software developer, the LBS and the network operator and government [32]. Second, the boundary between Cell (3) and (4) is fuzzy. Government institutions often cooperate with private corporations. The US National Security Agency (NSA) obtained direct access to the systems of Google, Facebook, Apple and other big tech companies, as part of the Prism program, which allowed NSA officials to collect material including search history, the content of emails, file transfers and live chats [33]. Nevertheless, the four ideal types of relations help us draw a rough grid into which finer resolution grids may be inserted in future iterations.

In Cell (1), two humans (Alice and Bob) are interacting face to face in a private or public space. This is the archetypal human-to-human interaction. Both Alice and Bob are conscious of being observed by each other and other humans, and have similar privacy goals—to uphold a tacit social code, the 'right and duty of partial display.' The sociologist Erving Goffman [34] described how all humans reveal personal information selectively to uphold this code, while constructing their public personae. Hence, the low incongruity between Alice's and Bob's goals to protect their privacy—both strive to uphold this tacit social code, to protect (or curate) their public personae, but also modulate it gradually over time, as the relation expands or shrinks. As Fried [35] explains, Alice may not mind that Bob knows a general fact about her, and yet feel her privacy invaded if he knows the details. For instance, Bob may comfortably know that Alice is sick, but it would violate her privacy if he knew the nature of the

illness. Or, if Bob is a good friend he may know what particular illness Alice is suffering from, but it would violate her privacy if he were actually to witness her suffering. Both control their behavior and the knowledge they share (outputs) about each other and may choose to modulate them over time. Goffman's theory applies in settings where participants can see one another face to face, but it has implications for technology-mediated interactions, for example, in email security [28]. When emailing each other, Alice and Bob may choose from a continuum of strategies to safeguard their privacy depending on context. They may refrain from emailing, they may email each other but self-censor, they may delegate privacy protection to mail encryption and firewalls, or they can work socially and organizationally to make certain that members of their community understand and police norms about privacy [36].

Cell (2) describes the interaction of a human, for example, Alice, the research leader of a participatory sensing campaign, with a group of campaign participants (Bob, Carol, Dan, Eric, etc.). Goal incongruity between Alice and the group may be high, if the group members are not aware of possible breaches to their privacy and their implications. As campaign leader, Alice has a high ability to control outputs, behaviors of group members, as well as of machines, and takes a series of privacy-safeguarding measures for the entire group before, during and after the campaign, a strategy Kounadi and Resch [37] call 'geoprivacy by design.' They propose detailed privacy-preserving measures in four categories, namely, six measures prior to the start of a research survey, four measures for ensuring secure and safe settings, nine measures for processing and analysis of collected data, and 24 measures for safe disclosure of datasets and research deliverables. Table 2 provides illustrative examples in each category. Interestingly, measures to control human behavior include two subtypes: outreach measures, e.g., participation agreement, and measures of self-restraint, e.g., use of disclaimers, avoiding release.

Table 2. Examples of measures controlling the transformation process.

	Measures Controlling Human/machine Behavior and Outputs
Prior to start of campaign	human behavior (participation agreement, informed consent, institutional approval); outputs (define criteria of access to restricted data)
Security and safe settings	human behavior (assign privacy manager, train data collectors); machine behavior (ensure secure sensing devices, ensure secure IT system)
Processing and analysis	outputs (delete data from sensing devices, remove identifiers from data set)
Safe disclosure	outputs (reduce spatial and temporal precision, consider alternatives to point maps) human behavior (provide contact information, use disclaimers, avoid the release of multiple versions of anonymized data, avoid the disclosure of anonymization metadata, plan a mandatory licensing agreement, authenticate data requestors)

Cell (3) describes the interaction of Alice with a private corporation, as user of a location-based service (LBS), of which Google Maps is the most popular and commonly used. Alice volunteers her location to the LBS to get directions to a desired destination [32]. In this case, goal incongruity between Google and Alice is high, as we can see by comparing Alice's commitment to (location) privacy to Google's former executive chair Eric Schmidt. "*If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place.*" [38]. On the other hand, Alice's ability to control how her location information is used by the LBS to infer other information about her is low. As a EU citizen, she can rely on GDPR to (partly) control the behavior of the LBS provider. Another strategy is lodging a complaint to her national Data Protection Authority (DPA). DPAs are independent public authorities in each EU state that supervise the application of GDPR and handle complaints lodged

against violations of GDPR. Max Schrems, the Austrian lawyer and privacy activist, is the face of GDPR complaint-lodging. His non-profit None of Your Business (NOYB) lodged four complaints about the take-it-or-leave-it practices of Google, Instagram, WhatsApp, and Facebook, the day GDPR became enforceable. He claimed that the platforms force users' consent to terms of use and demanded damages of $8.8 billion. The French advocacy group La Quadrature du Net (LQDN) similarly filed 19 complaints. On 21 January 2019, the French National Data Protection Commission (CNIL) imposed a financial penalty of €50 million against the company Google LLC, in accordance with the General Data Protection Regulation (GDPR), for lack of transparency, inadequate information and lack of valid consent regarding the ads personalization.

Cell (4) describes the interaction of Alice with government institutions. Alice trusts that her government will respect her right to information privacy (thus goal incongruity is low) but may be in the dark regarding the transformation process, unless a whistleblower leaks a secret surveillance program (e.g., [33]) or the abuse of private data [39]. Further, if the public organization, where Alice works, engages in processing likely to result in a high risk to the rights and freedoms of individuals, Alice may lodge a complaint to the DPA and request a Data Protection Impact Assessment (DPIA). Such processing may include the systematic and extensive evaluation of personal aspects of an individual, including profiling, the processing of sensitive data on a large scale; or, the systematic monitoring of public areas on a large scale. She may even apply more covert techniques. The surveillance scholar Gary Marx [40], a student of Erving Goffman, outlined 11 behavioral strategies intended to privately subvert the collection of personal information and resist surveillance. He claims that

> "*in spite of doomsday scenarios about the death of privacy, in societies with liberal democratic, economic and political systems, the initial advantages offered by technological developments may be weakened by their own ironic vulnerabilities and [by] 'human ingenuity'*" ([40], p. 388).

Another strategy for Alice is collective, for example, participating in popular resistance to unpopular government action. When the government of the Federal Republic of Germany announced a national Census on April 27, 1983, German citizens protested so strongly that a dismayed German government had to comply with the Federal Constitutional Court's order to stop the process and take into account several restrictions imposed by the Court in future censuses. Apparently, asking the public for personal information in 1983, the fiftieth anniversary of the National Socialists' ascent to power, was bad timing, to say the least [41]. When the Census was finally conducted in 1987, thousands of citizens either boycotted (overt resistance) or sabotaged (covert resistance) what they perceived as Orwellian state-surveillance [42]. We should bear in mind that these remarkable events took place in an era where the government was the only legitimate collector of data at such a massive, nationwide scale and at a great cost (approx. a billion German marks). Nowadays, state and corporate surveillance are deeply entangled. In response, technologically savvy digital rights activists have been influential in several venues, including the Internet Engineering Task Force (IETF) and the Internet Corporation for Assigned Names and Numbers (ICANN), through the Non-commercial User Constituency (NCUC) caucus. Yet their efforts have largely remained within a community of technical experts ('tech justice') with little integration so far with 'social justice' activists [43].

3. The Transformation Processes of Our Data in the Context of Location Privacy

3.1. Data Types in Play

Having a *personal understanding* of one's location privacy requires an understanding of regulations in place, trust in regulation maintenance processes, as well as an understanding of the personal data that is in play, and the inference capabilities that others may have once they have access to such data. The regulations and their maintenance are important because they secure the boundary conditions, under which a person can attempt to understand her information vulnerability. Below, we define 'personal data' and provide a typology that helps to unravel the data in play. With that understanding,

we also address the mechanisms of inference over personal data, and possible countermeasures available to the various actors: those that volunteer the data and those that receive such.

According to the GDPR, Article 4(1) [44], personal data is "*any information relating to an identified or identifiable natural person*." One can distinguish between three types of personal data: *volunteered*, *observed* and *inferred*. The first type is typically explicitly handed over by the natural person 'as part of the deal'; the second type is captured by monitoring that natural person's actions and is much more stealthy in nature. The third type is created beyond the natural person's cognitive horizon. We remark that in the context of location privacy, these three types may involve both spatial and non-spatial data. We define spatial data as explicitly including location, i.e., information able to be interpreted in an open and well-known system with the interpretation leading to a location. Examples are map or GPS coordinates, postal codes and street addresses.

One needs to agree that we are running an urgent agenda in addressing location privacy concerns, because in this information age, and in this infoconomy, data sources are rapidly expanding and third-party inference capabilities show substantial growth. First of all, public domain geospatial base layers have drastically increased in volume, quality and geographic coverage, and thus, information once known as the yellow pages, the road infrastructure, or the land administration registry are now often online [45–47]. Such sources provide the background against which location intelligence gathering and interpretation is made fruitful.

Next, we are making use of many more online applications (smartphone, lap- and desktop) now than we were, say, five years ago, and that trend is not tailing off yet. Younger generations also consist of more intensive producers. Moreover, the net of 'natural person satellites' around us is increasing in density rapidly. Such satellites are entities in our vicinity with which, with some regularity, we share the same location: family members, colleagues and friends come to mind first. The majority of them are already in the 'data play' anyway. Developments in smart cities and the Internet-of-Things, are bringing inanimate satellites to the scene such as our refrigerator, our bike, car and car keys, our home thermostat, and our garbage can. These will all have an online presence, and their (sometimes static) location and operational state may inform third-parties of our own location, presence *and* absence, as well. Data security on these devices at present is alarmingly low [48].

Central to location privacy are data sources that associate with the person or with the location. Looking first at personal data, we recognize the following types:

unique identifier This is a data element that is associated with just one entity of interest; that entity may be a data subject or something else. This is a wide class of identifiers;

key identifier A data element that can be exploited with minimal effort to identify a (privacy-sensitive) data subject;

quasi-identifier A data element that almost discloses the identity of a data subject, due to its semi-unique value, and that will allow full disclosure when combined with other quasi-identifiers;

private attribute The remainder class of privacy-relevant but non-identifying data elements.

Key identifiers such as person names, phone numbers, email addresses, to some extent license plates and certain other device identity numbers, and also social media account names are all in this category. As the name suggests, quasi-identifiers do not immediately allow the identification of a data subject, and they require work. Key to quasi-identifiers is the aspect of data combinatorics. For instance, a combination of personal traits of athletes in a sports team may allow unique identification of some athlete. A private attribute represents information about a data subject that is exploitable to inference information about her. Alice may be known for her fondness of chai latte.

A useful typology regarding location data is one that splits out on the basis of data structure complexity. We recognize the following types ordered by increasing complexity:

location This is the base case and it provides the whereabouts of an entity, a data subject, or that of a data subject's activity;

location with co-variates A slight extension of the first case, in which the provided location is augmented with quasi-identifiers or private data elements. Such augmentation allows contextual inference about the function of the location to the data subjects;

timed location This is a next step up the ladder, and associates with any provided location also some form of time stamp. The combination of these data elements allows inferences towards what we can generically call trajectories. Presence and absence information also falls in this category;

timed location with co-variates The final case, which allows inference over entity or data subject activity trails and life cycles.

This typology is important because it implies levels of data richness that determine the caloric value of the data that fuels possible inference processes over them. The types hint at an important distinction in what can be inferred, and they warrant different levels of awareness with the data subject who volunteers the data.

3.2. Inference over Personal and Location Data

The exchange of personal and location data with third-parties commonly takes place in a service provision scenario. We use that term in a wide sense: local and national governments provide services to the citizens, software applications running on mobile and stationary devices (such as sensors and computing devices) provide services to the owners or holders. Adequate service delivery requires adequate data, and thus data processing, to serve appropriately. Alice understands that a driver's license renewal requires her to hand over identity and address details.

It is sensible to discriminate between controller and processor roles, as the GDPR does in its Article 4(7–8). The first determines purpose and means of processing, and the second 'just processes'. The key role of the controller is to define what is appropriate and adequate data in the context of some service delivery. In Figure 1, we sketch three common scenarios of service delivery. They differ in what happens to the personal and location data submitted by Alice in each scenario; they also indicate what Alice should know about data processing in each scenario.

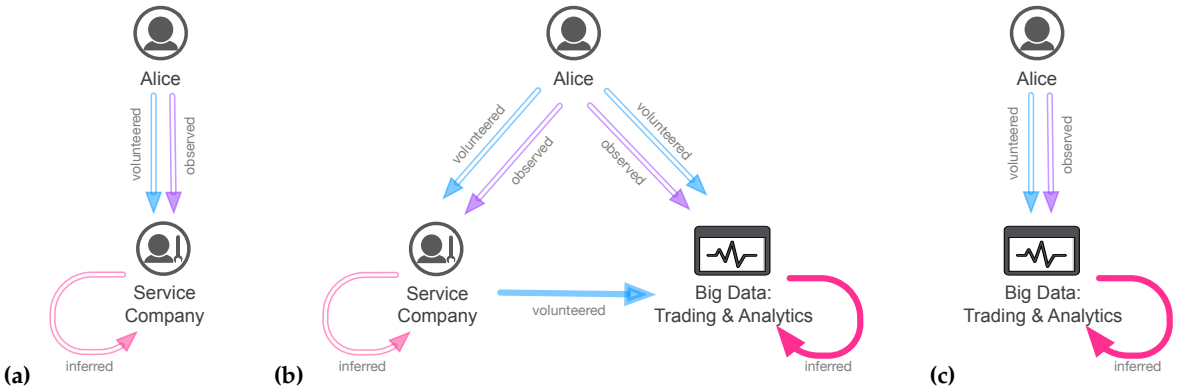

Figure 1. Three common scenarios in which Alice volunteers data with another party that provides some service: (**a**) An isolated service provision. (**b**) A service provision with 'unknown friend benefits'. (**c**) A 'full monty' service provision.

In the plain scenario of Figure 1a, the service is provided in an isolated setting, and the controller and processor are often the same entity. Data is processed to serve properly and optimally. Alice is advised to do a few things, in the context of her concern over location privacy when she considers making use of the service. First, she will want to know whether a DPIA has been carried out over this service provision and provider. She will also want to know whether alternative services exist. While some services are monopolistic, such as the driver's license renewal, others, such as a smartphone navigation application, are not. Navigation applications do exist in this first scenario category. A third

sanity check that Alice should carry out is to understand which personal data she is committing in the scenario, whether that data is needed for the functional purpose, and of the appropriate detail, and whether the service provider is building up user history and profile with the committed data. In this scenario, such is only legitimate when it aims to improve service quality levels to Alice. In principle, the user history, when purposeful, could be stored on Alice's device only.

The typical business model for the plain scenario depends on the controller type. When governmental, usually a small, fixed fee applies that can be seen as transaction cost; often government agencies have succeeded to economize their own processes and the service provision is seen as a win-win. When commercial, different modes exist, with one being a license fee for using the service that is either one-time and fixed, or that is subscription fee-based. Obviously, models also exist where Alice is offered to accept receiving advertisements against a lower, possibly zero, fee.

Many of the awareness questions that Alice must pose under scenario (a) remain valid in scenario (b). Much of what we wrote on scenario (a), applies here equally well. Yet, scenario (b) is more complex and typically also has a form of data hand-over by the service provider to the big data industry, consisting of data traders and data analytics companies. This is commonly part of the service provider's business model, and so Alice should think twice when receiving great service at low cost. She should also scrutinize the end-user agreement on what happens with her data after the service provider has handed over her data to a third party. This scenario has become much more common in recent years, due to the exponential growth of the big data markets. The situation is aggravated by Alice's potential engagement with big data market companies directly, for instance in using social media, or with providers of other services, which may also be enjoying a data hand-over agreement with the big data industry. The laws of data combinatorics imply that Alice is likely deeply personally profiled in such cases. She must remain on her guard for questionable business ethics.

The scenario of Figure 1c sketches a case where Alice has decided to use services directly from a big data entity. She may not be less disconcerted, but at least understands with which entity she is involved, and knows its reputation as a service provider and controller or processor. Were she less informed, she might perceive the service as the only of its type, and so consider its use inevitable. Luckily, Alice knows of alternative internet search engines, navigation apps, mail service providers, and so forth, for those situations when she cares about her location privacy. It is worth observing that where service providers operate in a competitive market, such as is the case in the telecom industry, big data companies are often known to be careful in location privacy handling.

One can justifiably pose the question whether Alice can distinguish between the sketched scenarios (a) to (c), let alone understand where her data ends up and which parties use it and to what end. At present, her information position is sometimes dire indeed, and if she finds it hard already, clearly others with a less strong background in information processing will be similarly uncertain. At present, they will need to rely on emerging regulations that bring transparency and on enforcing DPAs as well as consumer organizations that aim to keep parties honest, transparent and informed.

4. Privacy at the Cultural Level

In Sections 2 and 3, we focused on Alice's privacy, her goals and capability to safeguard it, and on the types of data that she is volunteering. We also discussed the possibly invading mechanisms of observation and inference that service providers and third parties may be applying. In so doing, we discussed privacy at the individual level, the first of Alan Westin's [16,18] three levels—individual, cultural and political. We placed Alice at the center of a typology linking her with her social environment. Alice safeguards the privacy of her research subjects as well as her own from attackers. She is capable of making use of the opportunities her legal environment provides to lodge formal complaints, when GDPR rules are broken. She is capable of overt and covert political resistance, when all other options seem futile. In this section, we discuss privacy at the cultural level, starting from a basic premise in social theory [49]: Alice's (privacy) preferences and commitments are shaped by

and shape the culture of her community and society. Her individual preferences and the culture—i.e., the shared beliefs, attitudes, or way of life, or world view—of the community or society in which she is socialized are deeply enmeshed and mutually reinforcing, with no way to decide which is the dependent and which the independent variable.

4.1. Cultural Theory: A Typology of Cultures

Social scientists have shown that the various ways in which individuals around the world express their preferences and commitments to human values, such as social justice, equality and privacy among others, are associated with four alternative ways of organizing human relations into cultures. Pepperday [50] offers a concise summary of these theories, each starting from different premises but arriving to similar ideal types of culture. The particular theory we use here goes back to the social anthropologist Mary Douglas and her fieldwork in the 1950s with the Lele people of the colonial Belgian Congo, now the Democratic Republic of Congo. Douglas' cultural theory distinguishes four ideal types of culture: egalitarianism, hierarchy, individualism and fatalism ([51], (1978)). For instance, egalitarians view social justice as just outcomes for all, hierarchists view justice as a just, rights-based process, while individualists view justice as just deserts—to each individual his due. Fatalists are resigned to a world of injustice they cannot control.

None of these four cultures is sustainable in pure form. Each culture needs more or less elements of the other three to become a viable hybrid. For instance, the individualist rule of 'notice and consent' fails to protect individuals' privacy. Neither do people read privacy notices, nor do they turn off the location tracking function of their cell phone. This leads to the "privacy paradox"—disclosing personal information, despite an expressed commitment to privacy [52]. Only a hierarchically reinforced form of consent can protect individualists from themselves. Article 7 of GDPR accomplishes this purpose. It

> "*requires affirmative consent, which must be freely given, specific, informed, and unambiguous. Consent can't be assumed from inaction. Pre-ticked boxes aren't sufficient to constitute consent*" [6].

The mix of individualism and hierarchy is an improvement over the choice to opt-out, that infers consent from inaction.

The dimensions of Douglas' typology of cultures are 'grid' and 'group' [53]. Grid measures the extent to which role differentiation constrains the behavior of individuals: where roles are primarily ascribed, grid constraints are high; where roles are primarily a matter of choice, grid constraints are low. Group, by contrast, measures the extent to which an overriding commitment to a social unit constrains the thought and action of individuals.

4.2. A Typology of Privacy Cultures

In the wake of the GDPR, all privacy cultures are readily observable. Fatalism, the most passive of the four, has been aggressively promoted by big tech companies for at least two decades. In 1999, Scott McNealy, the founder and CEO of Sun Microsystems, declared "you have zero privacy ... get over it," a statement some in the privacy industry took as tantamount to a declaration of war [54]. In 2009, when asked whether users considered Google a 'trusted friend,' former Google CEO Eric Schmidt responded, "*If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place.*" In 2010, Mark Zuckerberg claimed that the privacy social norm "*is just something that has evolved over time*" as people tend to share more personal information with more people [55]. Privacy fatalism among data subjects or consumers enables big tech companies to naturalize the massive extraction of personal data—conveniently labeled 'data exhaust'—and to duly appropriate it, much like the former colonial powers, who appropriated terra nullius or 'no man's land', and exploited it without legal interference [56]. The tech companies' extractivism is premised on formal indifference to the populations that comprise both their data sources and their ultimate targets for behavioral prediction, modification and monetization [9], as the Cambridge Analytica scandal [39] has shown. Besides fatalism, the three active privacy cultures—egalitarianism, individualism and hierarchy—are

clearly discernible in the EU. They share a common core—a commitment to data distributism, a more just distribution of benefits from data extraction (Table 3). We discuss each in turn using their most recent empirical manifestations in France, Germany and the United Kingdom.

Table 3. A typology of cultures ([51], (1978)).

		Grid	
		Weak	*Strong*
Group	*Strong*	Egalitarianism	Hierarchy
	Weak	Individualism	Fatalism

Individualists frame data privacy as a product that can be exchanged in the market place for a fair price (to each his due). An excellent example of this approach is the advocacy of the French think tank GenerationLibre [57] to extend the private property paradigm to personal data. GenerationLibre aspires to change the way the digital ecosystem works, by giving user-producers:

1. "*The possibility for e-citizens to negotiate and conclude contracts with the platforms (possibly via intermediaries) regarding the use of their personal data, so that they can decide for themselves which use they wish to make of them;*
2. *The ability to monetize these data (or not) according to the terms of the contract (which could include licensing, leasing, etc.);*
3. *The ability, conversely, to pay the price of the service provided by the platforms without giving away our data (the price of privacy?)*" (p. 7).

Hierarchists may be willing to surrender some of their privacy to a legal or rational authority (e.g., government) they trust, in exchange for another public good they value, for example, security or economic growth. Andrea Nahles [58], the Chairperson of the German Social Democratic Party, framed the problem thus:

> "*Empires like Google and Amazon cannot be beaten from below. No start-up can compete with their data power and cash. If you are lucky, one of the big Internet whales will swallow your company. If you are unlucky, your ideas will be copied.*''

Her solution is a Data-for-all law:

> "*The dividends of the digital economy must benefit the whole society. An important step in this direction: we [the state] must set limits to the internet giants if they violate the principles of our social market economy. [. . .] A new data-for-all law could offer decisive leverage: As soon as an Internet Company achieves a market share above a fixed threshold for a certain time period, it will be required to share a representative, anonymized part of their data sets with the public. With this data other companies or start-ups can develop their own ideas and bring their own products to the market place. In this setting the data are not "owned" exclusively by e.g., Google, but belong to the general public.*"

Yet, as Morozov (2018) argues, Nahles' agenda "*needs to overcome a great obstacle: citizens' failing trust in the state as a vehicle of advancing their interests*," especially in a country like Germany, with a long history of data privacy activism.

Instead Morozov [59] argues for an egalitarian approach to privacy as constitutive of who we are and as radical citizen empowerment.

> "*We should not balk at proposing ambitious political reforms to go along with their new data ownership regime. These must openly acknowledge that the most meaningful scale at which a radical change in democratic political culture can occur today is not the nation state, as some on the left and the right are prone to believe, but, rather the city. The city is a symbol of outward-looking cosmopolitanism—a potent answer to the homogeneity and insularity of the nation state. Today it is the only place where the idea of exerting meaningful democratic control over one's life, however trivial the problem, is still viable.*"

Similarly, the Oxford-based Digital Rights to the City group, proposes a deeper meaning to the right to information, a declaration that "*we will no longer let our information be produced and managed for us [presumably by the state or corporations], we will produce and manage our information ourselves*" [60].

We saw that in the wake of the GDPR, the 'new global digital gold standard' [12], privacy cultures are emerging that value privacy differently (Table 4):

1. as a tradeable private good in return for another private good,
2. as something that constitutes who we are, and therefore is unalienable,
3. as something to be delegated to a trusted father-state and traded with a public good, and
4. as something that does not exist anymore and we should get over with.

As cultural theory predicts, eventually hybrid privacy cultures will prevail in specific European communities and societies.

Table 4. A typology of privacy cultures.

		Grid	
		Weak	*Strong*
Group	*Strong*	Data distributism (egalitarianism) **Slogan**: We produce and manage our personal data **Privacy**: Personal data as unalienable, constituting the self	Data distributism (hierarchy) **Slogan**: Data-for-all law **Privacy**: Personal data as a good that may be traded with a public good
	Weak	Data distributism (individualism) **Slogan**: My data are mine, but I sell them for a fair price **Privacy**: Personal data as tradeable product.	Data extractivism (fatalism) **Slogan**: You have zero privacy, get over it **Privacy**: Zero

5. Personal Data Protection in the African Union: An Outlook

Throughout this study, we argued that the fundamentally different privacy cultures of EU and the US can be attributed to a clash of two core values, which has resulted in what some analysts call a "*transatlantic data war*" ([4], p. 117). On the one hand, we have a European interest in personal dignity, on the other hand, an American interest in freedom. "*On both sides of the Atlantic, these values are founded on deeply felt sociopolitical ideals, whose* histories *reach back to the revolutionary era of the later eighteenth century*" ([14], page 1219, emphasis added). This motivated us to explore (location) privacy and related safeguarding measures and strategies at two levels. First, at an individual level, with Alice as protagonist, a fictitious (geo)computing scientist safeguarding the privacy of her research subjects as well as her own from attackers; and second at a cultural level, by describing four data privacy cultures—egalitarian, hierarchist, individualist and fatalist—all of recent vintage and emerging within the EU in the wake of GDPR. We also noted that historically entrenched privacy cultures may inhibit exporting the GDPR as a one-size-fits-all approach to other countries, e.g., to Member States of the African Union (AU).

In this final section, we speculate about the challenges a group of African and European collaborators, working on a joint research project, should tackle, when its activities are likely to affect the (location) privacy of African 'data subjects' or their territorial assets, in a Member State of the AU. We use the word 'speculate' purposefully to emphasize that any such exploration is meant only to provoke deliberation, with other (geo)computing scientists who, like us, are routinely engaged with African academia and government officials in long-term collaborative research. Three issues merit attention in this regard: (1) African data protection legislation, (2) (data) privacy cultures within the AU, (3) the social construction of personal data.

First, we note that the broad territorial scope of GDPR implies that its articles are applicable to every non-EU organization that processes the personal data or monitors the online activities of EU citizens. Article 45(1) of GDPR regulates that the

> "*transfer of personal data to a third country or an international organization may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organization in question ensures an adequate level of protection*."

If the European Commission decides that an African country is ensuring an adequate level of data protection in processing data of Europeans, we may assume that the citizens of that country enjoy the same level of data protection. About 40% of African countries have enacted data protection legislation, which abides either to OECD standards (1st generation), or the EU DPD 1995 standards (2nd generation), or even features a few GDPR elements (3rd generation), according to Greenleaf and Cottier [61]. The latter refers to Mauritius, one of Africa's dynamic but small economies, which updated its 2004 law in 2017, with a new Data Protection Act 2017 featuring some GDPR elements. In June 2014, the African Union adopted the Convention on Cyber-security and Personal Data Protection, known as the Malabo Convention [62], the first treaty outside the EU to regulate the protection of personal data at a continental level [63]. The Convention aims to establish regional and national legal frameworks for cyber-security, electronic transactions and personal data protection, but its actual impact depends on ratifications, of which there were none by early 2016 [5]. In 2018, the AU created data protection guidelines, broadly aligned with the GDPR, for its Member States, with contributions from regional and global privacy experts, including industry privacy specialists, academics and civil society groups [62].

What could we expect from those AU Member States without any data protection legislation in place? As Makulilo [64], a Tanzanian privacy scholar, wryly observes,

> "*the major legal systems in Africa namely common and civil law legal systems which are Western in origin, create fertile grounds for adaptability of European law. While these systems were forcibly imposed on Africa by European countries during colonial rule as part of the colonial superstructure and an instrument of coercing Africans to participate in the colonial economy, they were inherited by African countries on independence. [. . .] Thus, the attitude to view these systems as colonial has diminished significantly as more customisation continues to take place. It is arguable that African countries are no strangers to the adaptation of 'foreign law'*." (p. 451).

Obviously, a law in place does not necessarily imply its enforcement. Only Kenya and South Africa have tested data protection rights in courts so far, an indicator of willingness to enforce the law [63].

Second, much has been made of Ubuntu, the famed African egalitarian culture, whose core definition 'people are people through other people' leaves little room for personal privacy, and is at odds with the strong western emphasis on individual rights. The South African information scientists Olinger, Britza and Olivier [65] submit that Ubuntu, while still inspirational in many spheres of life including African politics and business, has little purchase as a philosophical foundation of African data protection legislation. Instead, they recommend alignment with European data protection legislation on pragmatic grounds, especially for African countries for which the EU is a major data trading partner. Arguing differently, Makulilo [63] makes a similar claim. He suggests that urbanization, the influence of modern technologies and globalization have destroyed the social cohesion of communities, while individualism is the order of the day in urban Africa. He recommends that data privacy regulations should ensure the right to privacy of individual African citizens' is secured, much like it ensures the right of EU citizens. Further, we take for granted that the other three privacy cultures, and associated hybrids must exist as well (after all, Mary Douglas' cultural theory originated in her ethnographic work in the Democratic Republic of Congo). However, African data privacy cultures and surveillance mechanisms are undocumented, apart from few exceptions [66]. For instance, we do not know to what extent, data privacy fatalism, aggressively promoted by big tech

companies, has taken root in African societies and communities, as it has in the EU. What data justice scholars (e.g., [25,26]) have documented is the massive personal data extraction from African-based organisations, as well as the lobbying of multinational corporations and their advocates for greater data emission, personalization and centralization for expert analysis in advanced economies. It appears that corporations are becoming the *de facto* custodians of African personal data, while local governments are hollowed-out, their capacities depleted and local livelihoods are harmed.

Third, an individual's social environment influences what is deemed her personal data. If a society considers a given mode of personal behavior—for example, political opinion, sexual orientation, religious or philosophical beliefs, trade union membership—to be socially legitimate, only then is related data deemed personal. This social fact will affect efforts to harmonize data protection legislation across nations. Finally, as Alan Westin ([16], p. 433) noted

> "*debates over privacy are never-ending, for they are tied to changes in the norms of society as to what kinds of personal conduct are regarded as beneficial, neutral, or harmful to the public good. In short, privacy is an arena of democratic politics. It involves the proper roles of government, the degree of privacy to afford sectors such as business, science, education, and the professions, and the role of privacy claims in struggles over rights, such as equality, due process, and consumerism.*"

6. Conclusions

Personal data protection shelters the privacy of individuals and communities from efforts of commercial and government actors to render them fixed, transparent, and predictable. Privacy is foundational to the practice of informed and reflective citizenship. In the European Union, the GDPR protects personal data of natural persons to uphold human dignity in contrast to US legislation, which protects freedom, especially from intrusions by the state. The EU and US privacy traditions are founded on sociopolitical ideals, whose histories reach back to the later eighteenth century and have attracted the attention of hundreds of legal scholars, social scientists, computer scientists and mainstream media analysts. Compared to this massive scholarship and analysis of privacy and data protection across the Atlantic, we have very little systematic knowledge on African views on privacy and local interpretations of a universal right to privacy in the African Union, where the lack or weak enforcement of data protection legislation endangers the right to privacy and human dignity of African citizens. If a European Alice finds it difficult to distinguish between the scenarios (a) to (c), presented in Section 3, let alone understand where her data ends up and which parties use it and to what end, the African Alice's information position will be significantly direr. Future research must address the fundamental ethical dilemma confronting European–African consortia when they deploy innovative geospatial technologies in disaster-prone African cities. A balance must be found between the use of innovative geospatial technologies, premised on location, and the respect for local privacy cultures. Data protection rights should apply equally to Europeans and Africans, and to citizens around the world.

Author Contributions: For this work, conceptualization and discussion took part between Yola Georgiadou, Rolf A. de By and Ourania Kounadi. Investigation was conducted as a wide scan of the formal literature, and of the public media and online discussion fora by all authors. Original draft preparation was conducted by Yola Georgiadou, and she is the lead author for Sections 1, 4 and 5. Yola Georgiadou, Ourania Kounadi and Rolf A. de By collaboratively wrote Section 2. Rolf A. de By and Ourania Kounadi are the lead authors of Section 3. Review and editing was done by all authors equally.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Powles, J. The G.D.P.R., Europe's New Privacy Law, and the Future of the Global Data Economy. *The New Yorker*, 25 May 2018.

2. Hoofnagle, C.J.; van der Sloot, B.; Zuiderveen Borgesius, F. The European Union General Data Protection Regulation: What It Is And What It Means. *SSRN Electron. J.* **2018**, doi:10.2139/ssrn.3254511.
3. Hearn, A. Facebook moves 1.5bn users out of reach of new European privacy law. *The Guardian*, 19 April 2018.
4. Schwartz, P.M.; Peifer, K.N. Transatlantic Data Privacy Law. *Georget. Law J.* **2017**, *106*, 115–179, doi:10.3366/ajicl.2011.0005.
5. United Nations Conference on Trade and Development (UNCTAD). *Data Protection Regulations and International Data Flows: Implications for Trade and Development*; United Nations Publication, New York and Geneva, 2016.
6. Solove, D. Why I Love the GDPR: 10 Reasons. Available online: https://teachprivacy.com/why-i-love-the-gdpr/ (accessed on 6 February 2019).
7. Houser, K.A.; Voss, W.G. GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy? *Richmond J. Law Technol.* **2018**, doi:10.2139/ssrn.3212210.
8. Tiku, N. Europe's New Privacy Law Will Change the Web and More. *Wired Magazine*, 30 March 2018.
9. Zuboff, S. The secrets of surveillance capitalism. *FAZ.net*, 5 March 2016; Available online: https://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html
10. Searls, D. Brands Need to Fire Adtech. Available online: https://blogs.harvard.edu/doc/2017/03/23/brands-need-to-fire-adtech/(accessed on 6 February 2019).
11. Layton, R.; McLendon, J. The GDPR: What It Really Does and How the U.S. Can Chart a Better Course. *Fed. Soc. Rev.*, **2018**, *19*, 234–248.
12. Buttarelli, G. The EU GDPR as a clarion call for a new global digital gold standard. *Int. Data Priv. Law* **2016**, *6*, 77–78, doi:10.1093/idpl/ipw006.
13. Albrecht, J.P. Hands Off Our Data! Available online: https://www.janalbrecht.eu/wp-content/uploads/2018/02/JP_Albrecht_hands-off_final_WEB.pdf (accessed on 6 February 2019).
14. Whitman, J.Q. The two western cultures of privacy: Dignity versus liberty. *Yale Law J.* **2003**, *113*, 1151, doi:10.2139/ssrn.476041.
15. Chakravorti, B. *Why the Rest of the World Can't Free Ride on Europe's GDPR Rules*; Harvard Business Review, Boston, MA, USA, 2018.
16. Westin, A.F. Social and political dimensions of privacy. *J. Soc. Issues* **2003**, *59*, 431–453.
17. Reed, P.J.; Spiro, E.S.; Butts, C.T. Thumbs up for privacy?: Differences in online self-disclosure behavior across national cultures. *Soc. Sci. Res.* **2016**, *59*, 155–170, doi:10.1016/j.ssresearch.2016.04.022.
18. Westin, A.F.; Rübhausen, O.M. *Privacy and Freedom*; Atheneum: New York, NY, USA, 1967; Volume 1.
19. Keßler, C.; McKenzie, G. A geoprivacy manifesto. *Trans. GIS* **2018**, *22*, 3–19, doi:10.1111/tgis.12305.
20. Floridi, L. *The 4th Revolution*; Oxford University Press: Oxford, UK, 2014; doi:10.4404/Hystrix-22.1-4649.
21. Warren, S.D.; Brandeis, L.D. The Right to Privacy. *Harv. Law Rev.* **1890**, *4*, 193, doi:10.2307/1321160.
22. Mulligan, D.K.; Koopman, C.; Doty, N. Privacy is an essentially contested concept: A multi-dimensional analytic for mapping privacy. *Philos. Trans. R. Soc. A Math. Phys. Eng. Sci.* **2016**, *374*, 20160118, doi:10.1098/rsta.2016.0118.
23. Zook, M.; Barocas, S.; boyd, d.; Crawford, K.; Keller, E.; Gangadharan, S.P.; Goodman, A.; Hollander, R.; Koenig, B.A.; Metcalf, J.; et al. Ten simple rules for responsible big data research. *PLoS Comput. Biol.* **2017**, doi:10.1371/journal.pcbi.1005399.
24. Masser, I.; Wegener, M. Brave New GIS Worlds Revisited. *Environ. Plan. B Plan. Des.* **2016**, doi:10.1177/0265813516665619.
25. Taylor, L.; Broeders, D. In the name of Development: Power, profit and the datafication of the global South. *Geoforum* **2015**, *64*, 229–237.
26. Mann, L. Left to other peoples' devices? A political economy perspective on the big data revolution in development. *Dev. Chang.* **2018**, *49*, 3–36.
27. Fairfield, J.A.T.; Engel, C. Privacy as a public good. *Duke Law J.* **2015**, *65*, 385–457.
28. Agre, P.E.; Rotenberg, M. *Technology and Privacy: The New Landscape*; MIT Press: Cambridge, MA, USA, 1997; doi:10.1353/tech.2000.0173.
29. Altman, I. Privacy regulation: Culturally universal or culturally specific? *J. Soc. Issues* **1977**, *33*, 66–84.
30. Ouchi, W.G. A Conceptual Framework for the Design of Organizational Control Mechanisms. *Manag. Sci.* **1979**, *25*, 833–848, doi:10.1287/mnsc.25.9.833.

31. Ciborra, C.U. Reframing the Role of Computers in Organizations—The Transactions Cost Approach. *Off. Technol. People* **1987**, *3*, 17–38, doi:10.1108/eb022640.
32. Herrmann, M. Privacy in Location-Based Services; Privacy in Locatie-Gebaseerde Diensten. Ph.D. Thesis, Katholieke Universiteit Leuven: Leuven, Belgium, 2016.
33. Greenwald, G.; MacAskill, E. NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*, 7 June 2013.
34. Goffman, E. *The Presentation of Self in Everyday Life*; Anchor Books: New York, NY, USA, 1959; Volume 5.
35. Fried, C. Privacy. *Yale Law J.* **1968**, *77*, 475–493.
36. Bowker, G.C.; Baker, K.; Millerand, F.; Ribes, D. Toward Information Infrastructure Studies: Ways of Knowing in a Networked Environment. In *International Handbook of Internet Research*; Springer Netherlands: Dordrecht, The Netherlands, 2009; pp. 97–117, doi:10.1007/978-1-4020-9789-8_5.
37. Kounadi, O.; Resch, B. A Geoprivacy by Design Guideline for Research Campaigns That Use Participatory Sensing Data. *J. Empir. Res. Hum. Res. Ethics* **2018**, *13*, 203–222, doi:10.1177/1556264618759877.
38. Newman, J. Google's Schmidt Roasted for Privacy Comments. *PC World*, 11 December 2009.
39. The Guardian. The Cambridge Analytica Files. Available online: https://www.theguardian.com/news/series/cambridge-analytica-files (accessed on 2 February 2019).
40. Marx, G.T. A Tack in the Shoe: Neutralizing and Resisting the New Surveillance. *J. Soc. Issues* **2003**, *59*, 369–390, doi:10.1111/1540-4560.00069.
41. Anonymous. Datenschrott für eine Milliarde? *DER SPIEGEL*, 16 March 1987.
42. Anonymous. Volkszählung: "Laßt 1000 Fragebogen glühen". *DER SPIEGEL*, 28 March 1983.
43. Dencik, L.; Hintz, A.; Cable, J. Towards data justice? The ambiguity of anti-surveillance resistance in political activism. *Big Data Soc.* **2016**, doi:10.1177/2053951716679678.
44. European Union. *Regulation (EU) 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)*; European Union: Brussels, Belgium, 2016.
45. De Graaff, V.; de By, R.A.; van Keulen, M. Automated Semantic Trajectory Annotation with Indoor Point-of-interest Visits in Urban Areas. In Proceedings of the 31st Annual ACM Symposium on Applied Computing, Pisa, Italy, 4–8 April 2016; pp. 552–559, doi:10.1145/2851613.2851709.
46. Haklay, M.; Weber, P. OpenStreetMap: User-generated street maps. *IEEE Pervasive Comput.* **2008**, *7*, 12–18.
47. Cetl, V.; Tomas, R.; Kotsev, A.; de Lima, V.N.; Smith, R.S.; Jobst, M. Establishing Common Ground Through INSPIRE: The Legally-Driven European Spatial Data Infrastructure. In *Service-Oriented Mapping*; Springer International Publishing AG, *sine loco*, 2019; pp. 63–84.
48. Matthews, K. The Current State of IoT Cybersecurity. Available online: https://www.iotforall.com/current-state-iot-cybersecurity/ (accessed on 6 February 2019).
49. Barnes, B. *The Elements of Social Theory*; Princeton University Press: Princeton, NJ, USA, 2014.
50. Pepperday, M.E. Way of Life Theory: The Underlying Structure of Worldviews, Social Relations and Lifestyles. Ph.D. Thesis, Australian National University, Canberra, Australia, 2009.
51. Douglas, M. *CulturaL Bias. in the Active Voice*; Routledge and Kegan Paul: London, UK, 1982.
52. Regan, P.M. Response to Privacy as a Public Good. *Duke Law J.* **2016**, *65*, 51–65.
53. Thompson, M. *Organising and Disorganising. a Dynamic and Non-Linear Theory of Institutional Emergence and Its Implication*; Triarchy Press, Devon, UK, 2008.
54. Sprenger, P. Sun on Privacy: 'Get Over It'. *Wired News*, 26 January 1999.
55. Johnson, B. Privacy no longer a social norm, says Facebook founder. *The Guardian*, 11 January 2010.
56. Couldry, N.; Mejias, U.A. Data colonialism: Rethinking big data's relation to the contemporary subject. *Telev. New Media* **2018**; doi:10.1177/1527476418796632
57. Landreau, I.; Peliks, G.; Binctin, N.; Pez-Pérard, V. My Data Are Mine. Available online: https://www.generationlibre.eu/wp-content/uploads/2018/01/Rapport-Data-2018-EN-v2.pdf (accessed on 3 February 2019).
58. Nahles, A. Die Tech-Riesen des Silicon Valleys gefährden den fairen Wettbewerb. *Handelsblatt*, 14 August 2018.
59. Morozov, E. There is a leftwing way to challenge big tech for our data. Here it is. *The Guardian*, 19 August 2018.

60. Shaw, J.; Graham, M. An Informational Right to the City? Code, Content, Control, and the Urbanization of Information. *Antipode* **2017**, *49*, 907–927, doi:10.1111/anti.12312.
61. Greenleaf, G.; Cottier, B. Data Privacy Laws and Bills: Growth in Africa, GDPR Influence. In *152 Privacy Laws & Business International Report*; Number 18–52 in UNSW Law Research Paper; University of New South Wales: Sydney, Australia, 2018; pp. 11–13.
62. African Union. *African Union Convention on Cyber Security and Personal Data Protection*; African Union: Addis Ababa, Ethiopia, 2014.
63. Makulilo, A.B. A Person Is a Person through Other Persons—A Critical Analysis of Privacy and Culture in Africa. *Beijing Law Rev.* **2016**, *7*, 192–204, doi:10.4236/blr.2016.73020.
64. Makulilo, A.B. "One size fits all": Does Europe impose its data protection regime on Africa? *Datenschutz Und Datensicherheit* **2013**, *37*, 447–451.
65. Olinger, H.N.; Britz, J.J.; Olivier, M.S. Western privacy and/or Ubuntu? Some critical comments on the influences in the forthcoming data privacy bill in South Africa. *Int. Inf. Libr. Rev.* **2007**, *39*, 31–43.
66. Donovan, K.P.; Frowd, P.M.; Martin, A.K. ASR Forum on surveillance in Africa: Politics, histories, techniques. *Afr. Stud. Rev.* **2016**, *59*, 31–37, doi:10.1017/asr.2016.35.