Information without borders: towards a framework for extra-territorial respect for the right to privacy

Paul Hayes
Irish School of Ecumenics,
Trinity College Dublin,
Room 2.10, College Green,
Dublin 2, Ireland
Email: hayesp4@tcd.ie

Abstract: Informational de-territorialisation is making the right to privacy more vulnerable as communications pass through international borders or are susceptible to mining when published on the internet. A factual relationship emerges where states acquire personal data relating to non-citizens outside of their territory, which triggers a fiduciary relationship that makes the state responsible for the respect of the non-citizen’s right to privacy, and for ensuring that right, which remains subject to legitimate limitations or derogations.

Keywords: fiduciary theory; privacy; extra-territorial; technology; information ethics; human rights.


Biographical notes: Paul Hayes is currently a PhD candidate in the Irish School of Ecumenics, Trinity College Dublin, working on a thesis entitled ‘An analysis of emerging human rights and ethical issues in the harvesting of data from social media during emergency response to natural hazards’, under funding from the EU FP 7 funded Slándáil Project.

1 Introduction

The rapid advances in information and communication technologies (ICTs) in recent decades have seen an exponential increase in the availability and accessibility of information. We are sliding from an industrial historical era into one of hyperhistory – an age of information abundance where societies and economies are shifting from production and consumption of material goods and services to ones which are also reliant upon and driven by digital goods and services, and their supporting infrastructure. Communications across the globe are instantaneous. Social media services such as Facebook and Twitter connect billions (Statista, n.d.). One result of our increasing interconnectedness is an informational de-territorialisation, one which presents challenges for Westphalian paradigm of state sovereignty (Floridi, 2015; Pagallo, 2015). Global data flows are near boundless and actions executed in one state can produce
effects in another. ‘Cyberspace’ has changed the nature of threats to state security as attacks can be projected with ease, and ostensibly without violence, against infrastructure abroad (recall stuxnet, for instance). As well as creating threats for national security, however, it has also created opportunities for its protection, opportunities which are not without implications for human rights.

Though argued to be a res communis and characterised as being similar to international waters in its nature, and seeing some naively pronounce its independence from the sovereign control of states, the ethereal construct remains rooted to physical existence (Jensen, 2015; Oates, 2015; Barlow, 2016). The infrastructures that support cyberspace – fibre optic cables, servers and more – still exist within the tangible world, within state boundaries, as do the people who use them (von Heinegg, 2013). The usage of such infrastructure is ultimately governed by national law, and rules of storage, access and transmission of data that reside on hard disks sitting within national boundaries are within the provenance of the hosting state. Data flows are global and information relating to one person can flow without resistance through porous borders and accumulate on servers across the world, across jurisdictions and subject to a plurality of laws. Recent revelations in the form of the US National Security Agency’s PRISM and the UK’s Government Communications Headquarters’ (GCHQ) Tempora programmes provide evidence that states have advanced capabilities in the interception, collection and analysis of digital communications in the service of the national security (Margulies, 2014; Shubber, 2013). These revelations of state surveillance powers have already catalysed pending litigation in the European Court of Human Rights.

Such technologies are notable for their ability to collect data which, previously, internet service users might have believed was safe from intrusion. Less intrusively, states can utilise publicly available information as it appears in social media, such as from Twitter feeds. This is proving a burgeoning source of information, for example, during emergency for emergency managers (Latonero and Shklovski, 2011), and technology is under development that allows the information present on it to be processed and analysed with a view towards isolating relevant information during crisis situations (Ashktorab et al., 2014; Imran et al., 2014) – the implication of the automated processing of information from this source, often laden with personal information, is also an interference with the right to privacy.

As states utilise privacy intrusive technologies (PITs) of varying levels of intrusion, interesting jurisdictional problems begin to emerge. As a state processes communications, whether passively should it be monitoring public social media feeds, or rather aggressively should it be accessing private communications or other sensitive data (emails, private messages, GPS data, etc.) it is interfering with the right to privacy. What is more, is that the state is potentially passively or aggressively interfering with the privacy of persons located outside of its territory. In human rights practice, the issue of extra-territorial jurisdiction is a contentious one, and in light of the power that states can project into ‘cyberspace’ to interfere with the rights of non-nationals living outside of their territory, a theory of jurisdiction must be elucidated in order to establish the responsibilities of states towards persons whose rights are being impacted, where conservative readings of the extra-territorial obligations of states would indemnify them against any responsibility at all. A conservative view of a state’s extra-territorial obligations to persons located outside of its physical territory is untenable in a world under-going a de-territorialisation of communications and data flows.
This article will seek to contribute to the discourse on the right to privacy and its extra-territoriality in the digital age, in the encroaching state of ubiquitous hyperhistory. Firstly, the consulted theories will be outlined. It will be argued, upon reviewing the restricted access and limited control, privacy as contextual integrity, and the ontological theory of privacy, that the right to privacy is a right to the appropriate flow of information, and that inappropriate flows that challenge our autonomy are an aggression against our person. Secondly, fiduciary theory, a constitutional theory, will be outlined and argued to be of import in resolving human rights problems through a frame of a fiduciary-beneficiary relationship between state and subject. This article will examine jurisprudence concerning extra-territorial obligations of states as well as the right to privacy, and use insights from privacy theory and fiduciary theory to offer coherence to a contentious area susceptible to ambiguous and uncertain conclusions, ultimately arguing – contrary to some international case law and traditional understandings of the concepts – that states have a negative obligation not to unduly interfere with the privacy of all persons (regardless of their physical location) whose data is within their sphere of power, and a responsibility to protect all personal data within their jurisdiction.

2 The ethics of privacy, a context sensitive right

Before proceeding it is essential to unpack a theory of privacy that both describes it as a condition and has a strong normative dimension that indicates with sufficient clarity when it has been violated. Before beginning the task of ascertaining the responsibility of states to citizens in their respect for the right to privacy in the domain of human rights, it is instructive to examine the core of its moral and philosophical nature, working from the assumption, as will be explored in the following section, that the nature of the state-subject relationship is an inherently moral one and one which should be guided by moral as well as legal principles. Furthermore, in a world where technology is changing the nature of privacy threats (and opportunities) (Floridi, 2005), it is essential to outline a theory of privacy that is fit for purpose in a new global context where it may have more nuance than simply being, ‘the right to be let alone’ [Warren and Brandeis, (1890), p.195].

The privacy debate has generated a wealth of scholarly material, seeing sometimes complementary and other times contrasting views on the nature of privacy emerge. Modern scholarly work on the right to privacy frequently focuses on privacy as a concept relating to access and control of personal information. This is in contrast to older approaches to the topic, which analysed privacy in terms of non-intrusion (the right to be free from unwarranted government intrusion) and seclusion (the right to be left alone, where perfect seclusion is perfect privacy), which Tavani (2007) argues were flawed in conflating the privacy with other concepts. Tavani (2007) argues that the non-intrusion interpretation conflates privacy with liberty – they are both closely related but distinct concepts, privacy enables liberty but they are not the same. On the other hand, the seclusion interpretation conflates privacy with solitude, that complete isolation is perfect privacy (Tavani, 2007).

Such theories are intricately bound to the historical, industrial period and are beholden to the idea of physical access being required for violations of privacy to occur (Tavani, 2007). More recent theories, such as Tavani and Moor’s theory of restricted access and limited control, Nissenbaum’s contextual integrity of information and
Floridi’s ontological theory of privacy re-orient the discourse to a more nuanced examination of access to and control of personal information and the conditions under which one can reasonably expect to lose privacy without it necessarily being violated. These three theories are discrete though not necessarily incompatible. In essence these theories attempt to clarify appropriate privacy expectations for different stages of the information life cycle, defined by Floridi (2014, p.6) as constituting phases of:

...occurrence (discovering, designing, authoring, etc.), recording, transmission (networking, distributing, accessing, retrieving, etc.), processing (collecting, validating, merging, modifying, organizing, indexing, classifying, filtering, updating, sorting, storing, etc.), and usage (monitoring, modelling, analysing, explaining, planning, forecasting, decision making, instructing, educating, learning, playing, etc.).

The RALC theory of privacy consists of three components that provide an account of the concept of privacy, its justification and its management (Tavani, 2007). In RALC a person has privacy from others where, in a given situation, they are protected from unauthorised intrusion, interference and information access by others (Tavani, 2007) – situation is left ambiguous though might be more fruitfully be considered context. Under the RALC account, a person can be in a naturally private situation or normatively private one (Tavani, 2007). In a naturally private situation a person is shielded from intrusion or access by physical boundaries – privacy can be lost though not violated as they are situations where no norms exist to protect the right to privacy (Tavani, 2007). Under the normatively private situation, norms (social, ethical and legal) regulate privacy loss – such situations include examples such as voting, confessions, or medical records (Tavani, 2007). The primary distinguishing factor between these two types of privacy is that in the former privacy can be lost but not violated as no norms exist to protect it, whereas in the latter privacy can be both lost and violated, as norms regulate control and access in particular contexts (Tavani, 2007). RALC proposes that complete informational control (about oneself) is impossible, but normative zones exist that protect information within particular contexts and that essentially control (in terms of choice, consent, and correction) commensurate with that context is important for the management of privacy (Tavani, 2007).

Nissenbaum’s thesis is that a right to privacy is not a right to secrecy or control, but a right to the appropriate flow of information [Nissenbaum, (2009), p.127]. In Nissenbaum’s framework of contextual integrity, context relative informational norms are characterised by the parameters of contexts (the particular situation/milieu), actors (senders, recipients and subjects) attributes (information types) and transmission principles (constraints on flow) (Nissenbaum, 2009). Nissenbaum (2009, pp.140–147), like Tavani and Moor, in her work does not conflate privacy with any other value or concept, but recognises its importance is in realising contingent values and rights – that the appropriate flow of personal information is necessary for self-determination, freedom from informational harm and injustice, the preservation of relationships and more.

A cornerstone of Nissenbaum’s (2009) work is its concern with the paradox of privacy in public spaces – which is very relevant here when one considers the collection of data from publicly available sources (for example Twitter or Facebook). Nissenbaum (2009) rejects the validity of the public/private dichotomy as a normative foundation for the concept of privacy – that persons should have an expectation to some degree of personal informational protection even when they are in public spaces, and this
expectation should not be restricted to conventionally private spaces such as the home. Nissenbaum (2009) ultimately argues, like Tavani and Moor, that appropriate information flow is context dependent, and the established norms of the context determine the appropriate information flow. Where a departure in the established norms has occurred, contextual integrity has been affected, a privacy violation has occurred (Nissenbaum, 2009).

The third approach to privacy is the most radical and merits special attention here due to its focus on the ontological status of privacy and the person. Floridi’s (2005) ontological theory of privacy is a product of his work on the philosophy and ethics of information. Floridi’s (2005, p.195) contention is that human beings (as well as reality in general) are informational in nature – that their personal information is not merely their property but is essentially a part of them, it belongs to them in the sense of ‘constitutive belonging’, or, a person quite simply is their information. Floridi (2005) argues that informational privacy is a product of ontological friction in the environment, which is a term for obstacles to information transmission (or transmission constraints). The greater the ontological friction there is in an environment, the less is known about someone, the less there is, the more there is known about somebody (Floridi, 2005). A glasshouse for example, would represent an environment with little ontological friction (Floridi, 2005). By Floridi’s account personal information is intrinsically part of our personal identity, and any unauthorised cloning or duplication is not comparable to theft so much as it is abduction (Floridi, 2005). After all, theft entails the removal of an object from a person’s possession, however information cannot be stolen, only replicated (or destroyed as the case may be) [Floridi, (2005), p.195]. Some privacy may be yielded in some instances if there is a beneficial trade-off; Floridi (2005) uses the example of biometrics where access to biometric information is yielded by a person in exchange for greater security. Floridi (2005) argues that losses of some basic information may not be a violation of privacy; we shed some information as we do skin, and some information is so generic and public that it can be shared without issue (public personal information, such gender or ethnicity for example) [Floridi, (2013), p.256]. The problems run deeper when disparate and seemingly innocuous data are aggregated together. Small-scale privacy losses from disparate pieces of information are natural, however large-scale aggregation of this information may advance an acceptable loss to a violation of our privacy, or an ‘aggression’ against our personal identity [Floridi, (2005), p.194; 2013]. In this account, a level of control or protection of our information is important for respect for our autonomy and self-determination, if not the core of our being – it arguably holds both intrinsic and extrinsic value.

These three accounts are discrete but comparable if not by nature at least by implication, and by taking the most salient aspects of each, a more comprehensive account of the condition and right to privacy can be established that will aid in attempting to resolve some problems in the following sections. Taken alone, each account of privacy has weaknesses. RALC’s suggestion of naturally private spaces is problematic and should not be mutually exclusive with normatively private situations, for even when one’s privacy is naturally shielded, that does not imply that norms are not also operational in that situation – the two are not mutually exclusive. Nissenbaum’s contextual integrity provides a robust account of privacy, whereby privacy is violated with departures from norms, though it is prescriptively somewhat thin in deference to existing norms, without providing tools for challenging them. Floridi’s ontological theory of privacy suffers from
some ambiguity, providing an excellent foundation for the sheer value of privacy to the person in its framing of personal information in terms of constitutive belonging; however, it is also prescriptively muddy even if in its guidance of intuition, it is a useful tool of phronesis.

Lessons can be learned from these three accounts of privacy, however. The three accounts of privacy support an understanding that a situation of perfect privacy is elusive if not impossible. Privacy loss is natural as we, or our information, are almost always accessible to varying degrees in different contexts. Privacy should be understood as [as Nissenbaum (2009) argues] a right to the appropriate flow of our information. The appropriate flow of information is governed by norms (ethical, social, legal) (Tavani, 2007; Nissenbaum, 2009). These norms governing a legitimate flow of information may often entail mechanisms that grant a person some degree of control over the flow, that is, provide for an element of management of their information (norms of choice, consent and correction). Different contexts may entail higher or lower degrees of ontological friction ( moderated by norms, the environment and types communication media) where more or less personal information is revealed and its transmission controllable. Our freedom is always circumscribed by external factors; it was Jean-Jacques Rousseau who said “[m]an is born free, and is everywhere in chains” [Rousseau, (1974), p.8] our unfettered agency is always limited by our environment, whether it is physical (or digital, as the case may be), or normative – if we truly are our information, if it is intrinsic to our being – then our control over that, just as it is with our bodies, is limited by our normative situations. However, the value of privacy – as itself a value on which many others are contingent, which gives us the ability to develop our identities and relationships – is of great importance and any interference must be executed with deliberation.

Normless situations may pose an additional challenge for the right to privacy too, and this will be addressed in due course.

3 Fiduciary theory, human rights and their limits

In this section, the constitutional theory fiduciary theory will be outlined and presented as an instructive theory for delineating the human rights responsibilities of states as well as the limits of their power.

The thesis of fiduciary theory is that the state and its agencies are fiduciaries of the people (legal subjects) whose interests they represent, and are entrusted with their authority by law to exercise power on behalf of the people (Fox-Decent, 2011). The state’s claim to legitimate authority requires it to respect the dignity and agency of its people (Fox-Decent, 2011). The principal function of the state is to provide a regime of secure and equal freedom under the rule of law (Fox-Decent, 2011). Intrinsic to providing a regime of secure and equal freedom is the provision of conditions of non-instrumentalisation and non-domination, therefore people are not to be treated as means but rather ends and are to be protected from arbitrary power (Fox-Decent, 2011). Human rights form the ‘blueprint[s]’ of this regime, entailing positive obligations to fulfil rights and negative obligations not to violate them [Fox-Decent and Criddle, (2010), p.315]. Human rights are constraints on unfettered exercises of state power and constitutive of a regime of secure and equal freedom. Human rights under fiduciary theory are defined by several characteristics [Fox-Decent and Criddle, (2010), p.302]:
they are relational and institutional in that they are responses to threats that emerge in the relationship between state (the institutions thereof) and subject

they are legal and non-positivist, constituting the necessary conditions of legal order under Kant’s theory of right

they are practical, seriously regarding rights enshrined in international human rights instruments

they are aspirational and universal, because they are necessary to ensure conditions of secure and equal freedom

they are deliberative, because they can be refined under democratic deliberation.

In addition to these defining characteristics, three desiderata further contribute to the substance of human rights [Fox-Decent and Criddle, (2010), p.318]:

- **Integrity** – “…human rights must have as their object the good of the legal subject rather than the good of the state’s officials”.

- **Formal moral equality** – “the fiduciary state owes a duty of fairness or evenhandedness to legal subjects because they are separate person’s subject to the same fiduciary power. Human Rights therefore, must regard individuals as equal cobeneficiaries of the fiduciary state”.

- **Solicitude** – “…human rights must be solicitous of the legal subject’s legitimate interests because those interests, like the interests of the child vis-à-vis the parent, are vulnerable to the state’s non-consensual power”.

The authority of human rights is embedded in the nature of the fiduciary-legal subject relationship as necessary pre-conditions for the provision of a regime of secure and equal freedom, and as they are non-positivist, their authority does not flow from international treaties, that is, their authority is not established by state consent (Criddle and Fox-Decent, 2012). International treaties merely “…signal the international community’s best provisional estimate of the determinate contents of particular human rights norms and legal consequences of their breach” [Criddle and Fox-Decent, (2012), p.57]. International bodies, such as the United Nations Security Council, are secondary guarantors of human rights and themselves are in a fiduciary-based relationship with their member states (Criddle and Fox-Decent, 2012; Criddle, 2013).

Human rights are ‘presumptively mandatory’ under fiduciary theory, however it does support the practice of rights limitations or derogation from provisions of human rights treaties under specific conditions (Criddle and Fox-Decent, 2009). Jus cogens norms are the exception to derogation, the violation of such rights (such as freedom from torture or slavery) would be incompatible with the state’s obligation to provide conditions of non-instrumentalisation and non-domination (Criddle and Fox-Decent, 2012). Limitations to rights must be proportional to the ends sought for the limitation, and the limitation must be justifiable to the legal subject, from whom the state’s power flows (Criddle and Fox-Decent, 2012).

In times of crisis states may assume emergency powers and are entitled under the theory to derogate from treaty-based human rights obligations (Criddle and Fox-Decent, 2012). Restrictions and limitations of rights during emergency must be consistent with the particular exigent demands of the emergency and proportional to the ends sought
(Criddle and Fox-Decent, 2012). Rights can be restricted or limited if the enactment of emergency powers is necessary to preserve the regime of secure and equal freedom and in times of existential threat, normal laws and ordinary restrictions may be inadequate to meet the exigencies of the situation (Criddle and Fox-Decent, 2012). For a state to declare an emergency a threat must be present or imminent, exceptional, and constitute a threat the organised life of a community as established in the European Court of Human Rights Lawless case (Criddle and Fox-Decent, 2012). A third criterion present in the Lawless case but omitted here is that an entire population must be threatened – fiduciary theory rejects this on the basis that the fiduciary obligation entails providing secure and equal freedom for all legal subjects and that a state can enact emergency measures when only a part of this community is threatened; failing this would be a failure to provide secure and equal freedom for this part of the community (Criddle and Fox-Decent, 2012).

Accountability to its legal subjects, from whom its power flows, is an essential aspect of the fiduciary relationship (Criddle and Fox-Decent, 2012). As such, the state is required to provide public justification for the measures taken during emergency as well as international notification to treaty bodies (Criddle and Fox-Decent, 2012). This provides avenues for subjects to contest the measures taken (Criddle and Fox-Decent, 2012). It bears emphasis that measures taken must be strictly necessary to address the exigencies of the situation and used only for the duration of the emergency (Criddle and Fox-Decent, 2012). Treaty derogation is therefore of a strictly temporary character, in contrast to ordinary limitations (consider prohibitions on hate speech) which can be of a permanent character. The principles governing entry into and conduct during emergency are broadly reflective of the Siracusa principles (UN Commission on Human Rights, 1984).

In international human rights law (or ‘international law’s emergency constitution’) there are occasionally conflicting norms and practices (Criddle and Fox-Decent, 2012). For a brief example, consider the ECtHR’s position on the Lawless case that requires an entire population to be under threat before an emergency can be declared, which directly contrasts with the position declared within the Siracusa principles that a threat to the life of a nation, warranting derogation, can include “…the whole of the population and either the whole or part of the territory of the state” (UN Commission on Human Rights, 1984; Criddle and Fox-Decent, 2012). Fiduciary theory can provide a coherent theoretical foundation for international law by providing a set of non-positivist, morally rooted principles grounded in a legal relationship between state and subject that are contingent on international human rights treaties or jurisprudence.

The fiduciary theory supports the argument that the state has the prerogative to act exceptionally under exceptional circumstances, an argument traceable to John Locke and one expounded upon by Carl Schmitt, whose positivist thinking on emergency powers took the idea of state prerogative to controversial extremes. Under Schmitt’s theory of exception, the state was not constrained by law in its response to emergencies, and exercised near unfettered power to address it (Schmitt and Strong, 2006). For Schmitt, it was deciding on the exception (or emergency), that proved the state’s sovereignty (Schmitt and Strong, 2006). For Schmitt, the law of normal times was inapplicable to the exception – the exception results in a normative lacuna (Schmitt and Strong, 2006). This highlights the concern that the exception can become the norm, and permanent emergency regimes can take effect (Gross and Ni Aolain, 2002); something which Agamben (2005) argues to be the contemporary paradigm of politics. When emergency
rule takes effect it can be difficult to terminate, emergency measures can become permanent law, or legal conditions of the exceptional state can become normalised (Gross and Ni Aolain, 2002). As Gross and Ni Aolain (2002, p.175) argue, “[e]mergency regimes tend to perpetuate themselves, regardless of the intentions of those who originally invoked them. Once brought to life, they are not so easily terminable”.

Fiduciary theory provides a normative framework that can stave off the excesses of the state in its response to emergencies, where human rights can be acutely vulnerable. It argues that the state does not wield unlimited power and that its power is to be used solely for the benefit of its legal subjects. It departs from the ideas of Schmitt in that the state does not exercise its power to protect itself, but to protect a regime of secure and equal freedom for its subjects. Its power is constrained by and directed by its adherence to human rights. Whilst emergencies may cause an unravelling of norms that challenge a state’s ability to address emerging challenges through conventional means, the state is not without forces that constrain its power. In a normative lacuna, legal principles still remain that compel and circumscribe state action (Criddle and Fox-Decent, 2012); it must continue to provide conditions of non-instrumentalisation and non-domination, for if it does not it loses its legitimate claim to power, which flows from the people.

With fiduciary theory and its implication for human rights outlined, as well as ethical theories establishing the condition and normative expectations surrounding privacy, it is time to move on to examine the right to privacy in international law and use these supporting theories to define acceptable limits to privacy as a human right.

4 Personal data and the limits of privacy as a human right

The right to privacy is protected in prominent international human rights treaties including the International Covenant on Civil and Political Rights and the European Convention of Human Rights. Article 17 of the ICCPR reads:

1 no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation

2 everyone has the right to the protection of the law against such interference or attacks.8

And Article 8 of the ECHR (the right to respect for private and family life):

1 Everyone has the right to respect for his private and family life, his home and his correspondence.

2 There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.9

The right is not absolute, as per wording of the text in each case, and can be subject to lawful interference.

It is instructive to examine case law of the European Court of Human Rights (ECtHR), of which there is a wealth of diverse cases, to outline the established limits of
In the case of the evolution of ICTs that enhance the state’s power over the information life cycle. The case law of the ECtHR has been significant in establishing norms for data capture, retention and disclosure. Such norms represent an exceptional class of norms, whereby standard expectations of privacy and the information lifecycle prove malleable in light of greater (public) interests.

The case law of the ECtHR extends comprehensive protection to personal data and demonstrates a cognisance of the importance of norms of a least consent and correction in its use by state agencies, but also the limits of these principles, which are governed by national security, public order, and other contexts.

The court has permitted rather significant interferences with the Article 8 right in terms of data collection, and permits interferences where they are in accordance with domestic law, justified and necessary and subject to safeguards. In an example of a particularly intrusive interference regarded as acceptable by the court, is Bernh Larsen Holding AS and Others v. Norway. In this case, the applicants’ server was accessed by the local tax authorities following an audit notification. The applicants’ system contained data not exclusively pertaining to its accounts, including staff email correspondences and personal information that was also not limited to the audited company’s business but also that of another business sharing the premises (upon challenging access the neighbouring business was also notified of an audit). Only a minor proportion of the information requested by the tax authorities was relevant to the tax audit. The court found that the state had been acting within its margin of appreciation and “...struck a fair balance between the applicant companies’ right to respect for ‘home’ and ‘correspondence’ and their interest in protecting the privacy of persons working for them, on the one hand, and the public interest in ensuring efficiency in the inspection of information provided by the applicant companies for tax assessment purposes, on the other hand”.

Surveillance activities are also standard practice conducted by law and order, and intelligence communities across the world. These constitute an interference with privacy, granting public authorities the ability to intercept varied (sometimes mundane and inconsequential) information about a subject. Surveillance has been tested and approved by the ECtHR. A pertinent case is that of Uzun v. Germany, where the applicant was the subject of substantial police surveillance including, crucially, of GPS data, which was the method later challenged in the courts. The applicant was subject to a criminal investigation related to several attempted murders and in order to prevent terrorist attacks. This case was notable in that the Court found the acquisition and use of GPS data less intrusive than other surveillance methods, and as such was not required to have safeguards as stringent as would be required for other methods (such as telecommunications interception), which would require defined limits to the surveillance period and procedures governing storage and use of information obtained. This surveillance was found to be pursuing legitimate aims, and the method was proportionate in light of the serious crimes under investigation.

The court has drawn lines in surveillance activities conducted by states. In the case of Roman Zakharov v. Russia the applicant complained to the court that Russia required mobile phone network operators to install equipment that enabled blanket interception of communications by the security and police services without judicial authorisation. The Court found in this case that there were insufficient safeguards protecting persons from abuse.
The case of Peck v. The United Kingdom provides an interesting case study in consent and disclosure of information obtained by authorities. Here, the applicant was recorded committing self-harm in a public location by closed circuit television cameras, the (unobscured) stills from the footage were subsequently released by the local authorities of the area as an example of the life-saving capabilities of CCTV. The photographic images were widely disseminated. An unjustified interference in Article 8 was found, particularly as no consent was given or attempts made to obscure the applicant’s identity in the first instance. The court found that the disclosures were not accompanied by sufficient safeguards and were therefore disproportionate and an unjustified interference. In this case, the acquisition of data from public spaces was not necessarily at issue; however, the disclosure of the information, without the applicant’s consent, was found to be a human rights violation.

In contrast, the case of Leander v. Sweden illustrates an acceptable interference of the right to privacy as regards disclosure. In this case the applicant was dismissed from his job in a naval base following a background check whereby his information was disclosed by the police to the armed forces. The information disclosed imparted that the applicant had formerly been a member of the Swedish Communist Party and a member of an association that published radical material, therefore he was considered a security risk in the context of his work. The court found that this interference had been lawful and within the state’s margin of appreciation as national security interests superseded individual liberty.

Transmission and disclosure of data however, must be strictly governed by adequate safeguards from abuse, as the case of M.M. v the United Kingdom demonstrated – where a violation of Article 8 was found whereby the applicant’s police caution for child abduction had been disclosed to a potential employer. Notably in this instance, the applicant provided consent to the disclosure but it was found that the applicant had no real choice as the employer had insisted on information pertaining to her criminal record. The rules governing data storage and disclosure relating to criminal records were found inadequate in this case, making no distinction between relevance and severity of crimes being disclosed and providing rare opportunity for deletion.

The Court has shown that data that is acquired by states is subject to deletion or correction by data subjects where it is incorrect or is unnecessary to hold. In Khelili v. Switzerland, a woman had been named as a prostitute in a police database, a claim which she contested. She requested removal of the term from her records but the police did not wholly comply. The court found that the storage of this information was harmful to the applicant’s reputation, especially with a view to the ease with which the data could have been transferred across authorities, and was not justified or necessary and that there had been an Article 8 violation.

The duration for which information on individuals can be maintained is a function of the purpose for which it is held. For example, in the cases of B.B. v. France, Gardel v. France and M.B. v. France the applicants complained about being included in a national sex offenders registry. In these cases, the court found no violation of Article 8. Inclusion in the database served a legitimate purpose of crime prevention and though the data was to be retained for a maximum of 30 years – opportunities for deletion requests were provided for. Clear conditions for access and disclosure of the information on the register were also in place in this instance.

The above cases represent a limited cross section of ECtHR case law, however they offer ample illustration of precedent. The right to privacy is circumscribed by contextual
demands – states have historically been granted a measure of latitude (in the case of the ECtHR, a doctrine known as the margin of appreciation) in their interferences with the right. The limits often apply to situations where national security and public safety are at risk, that is, so long as the interferences pursue a legitimate purpose. Interferences are required to be necessary, proportionate and lawful, and that law must be of a sufficient quality. Adequate safeguards from abuse must also be in place. The case law mitigates against indiscriminate collection and transmission of personal data, and against the retention of data in perpetuity. Interferences in the right to privacy represent a weaker normative environment whereby the autonomy of persons is constrained and their control over personal information is weakened.

The case law presented here broadly complies with the principles of fiduciary theory, interferences that were found to be legitimate by the court were done under conditions where there was a public need and if there had been no interference the states’ ability to provide a regime of secure and equal freedom would have been challenged. Interferences were found to be legitimate under conditions of adequate safeguards from abuse, which protected applicants from instrumentalisation or domination. As the measures were enacted out of necessity and were proportional to the ends sought, they were also justifiable to the public. Where measures were found to be violations of privacy, they were unnecessary, threatened instrumentalisation or domination, and were harmful for the dignity and autonomy of the applicants – they were not required for the state to discharge its fiduciary obligation of providing a regime of secure and equal freedom and actively cast the state itself as a threat to that regime. The case law also demonstrates an awareness of the importance of consent and control in the flow of information, though choice, in the context of discharging the fiduciary obligation, can fall to the periphery. An adherence to norms of consent and correction, so far as they are reasonable in a specific context, may be an instrumental component of safeguards from abuse that empower data subjects and can mitigate the possibility that they may be instrumentalised or dominated by the state.

The flow of personal information follows boundaries that are codified by the state – we do not have complete autonomy over our personal data much as we do not have complete autonomy over our own bodies; both are subject to countervailing forces that are presided over by the state in its construction of law, and are legitimate where they are necessary for the provision of conditions of non-instrumentalisation and non-domination. Necessary for these conditions to be met though, is a degree of reasonable influence over the life-cycle of one’s personal information; control that is commensurate with the context in which it is being used whether that is amendment or deletion of irrelevant records or the ability to stop inappropriate collection or transmission of personal data. For the interests of the state to be balanced accordingly against those of the individual, there must be appropriate safeguards, whether judicial or independent, in place to assist in the ethical and appropriate flow of information.

A puzzle still remains, one that represents a lacuna in human rights practice, which is to what extent do states owe fulfilment of the right to privacy to non-national persons not physically present within their territory or jurisdiction? Data collection programmes run by the NSA and GCHQ indicate that large volumes of data belonging to persons not within their respective state’s territories are exposed to interference. Communications that are typically not within the public domain are vulnerable to intrusion by powerful intelligence agencies. Personal data flows in abundance throughout public social media
feeds that are either volunteered or posted about unwitting subjects (information about third parties such as from photographs taken in public). This information is widely accessible to even the most rudimentary authorities that can monitor and duplicate it with ease.

This lacuna can be evidenced by the case of Weber and Sarvia v. Germany. This case concerned the extraterritorial telecommunications interception of a German journalist and an employee of Montevideo City Council by the Federal Intelligence Service. The German Government here used the argument that the application was “…incompatible ratione personae with the provisions of the Convention…” as both applicants resided in Uruguay and were therefore outside Germany’s jurisdiction. By that token, the government refused to accept that it owed any human rights obligations to persons outside of its jurisdiction in this instance. The application was found inadmissible and the ratione personae issue left unresolved, however it is an indicative example of the vulnerability of the personal data and privacy of persons located outside of a state’s jurisdiction when the state is willing to argue that it does not strictly owe them human rights obligations on this basis. For this reason, in the following the concepts and practice of territory and jurisdiction in human rights practice will be unpacked with a view towards establishing the extent of a state’s obligation to respect the right to privacy abroad.

5 Territory and Jurisdiction

There is contention surrounding the reach of a state’s duty to respect and fulfil human rights that stems from the wording of Article 2 of the ICCPR, that “[e]ach State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction without distinction of any kind…” and arising from Article 1 of the ECHR where “[h]igh Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section 1 of this convention”, [King, 2009; van Schaak, (2014), p.27]. There are three competing interpretations of the implications of the above quoted text.

The first interpretation is the narrow view that the state owes duties (positive and negative) only to individuals who are within both the jurisdiction and territory of the state (King, 2009; Margulies, 2014; van Schaak, 2014). The second is the protective view, whereby the state owes duties to two classes of people; those who are within the state’s territory, and those within its jurisdiction (King, 2009; Margulies, 2014; van Schaak, 2014). That is, a person may be located within the state’s territory but not its jurisdiction (for example, where the state does not have effective control over a portion of its territory). The third, emergent interpretation, the gestalt approach, is that the state holds positive obligations to ensure human rights over persons within its jurisdiction and territory, negative duties to respect the rights of persons “…without territorial limitation”, and must ensure human rights where it has the capacity to do so as defined by its relationship with individuals involved [van Schaak, (2014), pp.29, 48–49; Margulies, 2014].

The narrow view is problematic and is conducive to abuses of rights without any accountability – the population of foreign territories or jurisdictions outside of state control are owed neither positive nor negative duties (King, 2009).
International practice on extra-territorial application of human rights treaties has been divided. The Human Rights Council (HRC) adheres to a protective approach (Margulies, 2014), whereas the ECtHR has diverse case law that has gravitated towards a gestalt approach but has also shown deference to a narrow view. A brief examination of ECtHR case law is instructive to illuminate precedents regarding extra-territorial applicability of human rights law (HRL).

Much of the case law of the ECtHR pertaining to extra-territorial jurisdiction relates to situations of armed conflict and military occupation, but nonetheless remains a useful guide due to the generally applicable precedents that have emerged from it.

The court normally rules in favour of applications where it finds a cause and effect relationship between state and applicant or where the state is in effective control of the area held outside of its territory.

In the case of Loizidou v. Turkey the applicant was prevented from accessing her property in northern Cyprus as a result of the occupation by Turkish troops and the establishment of the Turkish Republic of Northern Cyprus (TRNC). The Court determined that due to Turkey’s significant military presence in the area of northern Cyprus and its support of the TRNC, it was responsible for the policies and actions of the TRNC, which fell within Turkey’s jurisdiction despite being outside of the territory of Turkey. Subsequent cases such as Cyprus v. Turkey and Manitaras and Others v. Turkey reaffirmed that Turkey was ultimately responsible for the actions of the TRNC and consequently owed the full range of treaty obligations to persons within the area controlled by the TRNC. The Court has found that states’ jurisdiction (and therefore human rights responsibilities) is invoked where states’ exercise authority and control, even in limited extra-territorial zones where that authority is active, such as in Ocalan v. Turkey where the state was found responsible for the human rights of the applicant after seizing him in a Turkish registered aircraft in an international airport in Nairobi.

The Court has also found that where a state executes an action in its own territory that produces an effect in another, a jurisdictional link is created. In Sericing v. the United Kingdom, the applicant faced murder charges and extradition to the USA where he would face conditions tantamount to a violation of Article 3, prohibition of torture or inhuman or degrading treatment or punishment. The Court found that in this instance, the UK would be responsible for any violation of his rights arising from extradition. Furthermore, in Andreou v. Turkey, the applicant claimed that she had been shot by Turkish troops, who opened fire from TRNC territory, whilst she was outside a UN buffer zone. The territory where she stood was not under Turkish effective control, however the act of firing on the applicant and others brought her within Turkish jurisdiction.

The Court has therefore found in numerous instances that a state was responsible for the human rights of persons outside of its territory and defined numerous instances where the state’s jurisdiction applies. Consistent with the narrow view, however, the Court has not found that state’s hold responsibilities outside of the territory of contracting parties to the ECHR. In the case of Bankovic v. Belgium and 16 Other Contracting States the applicants complained about a NATO bombing of a Serbian Radio and Television HQ situated in Belgrade that resulted in numerous fatalities. The Court decided that the victims in this instance were not within the jurisdiction of the respondent states as the site of occurrence of the bombing was not within the area of contracting parties. Similarly, though less decisively, in Saddam Hussein v. Albania and 20 other Contracting Parties, the infamous applicant complained of his arrest, detention and handover to Iraqi
authorities and subsequent trial, believing that he would be executed following a ‘show trial’. He argued that he was within the jurisdiction of the respondent states, which were occupying powers. The Court found no jurisdictional link as the applicant failed to support the level of involvement and power wielded by the respondent states.

In contrast, the HRC has been less concerned with physical location of a rights abuse than with the relationship between the applicant and respondent, as demonstrated in Lopez v. Uruguay (King, 2009). Whether the nature of this relationship is legal (the state exercises power lawfully), or factual (the state exercises its power with de facto competence) was left as an open question (King, 2009). King (2009) notes that jurisdiction conceived as applicable to persons in a legal relationship with a state only has been derided on the basis that states acting beyond their ‘lawful competence’ could violate human rights without accountability – such a scenario has been demonstrated in the ECtHR’s Bankovic case.

6 A fiduciary solution to extra-territorial action

Consulting fiduciary theory is an instructive start in attempting to resolve an appropriate approach to jurisdiction that leaves minimal gaps in human rights protection. Under this theory, the state is “…responsible to its subjects alone for the provision of domestic legal order” [Fox-Decent, (2011), p.109]. However, as demonstrated in the foregoing, the state has the capacity to exert irresistible discretionary power over non-subjects, that is, persons not within the state’s territory, subject to its de facto sovereignty. The law authorises the state to provide a regime of secure and equal freedom, but it does this on behalf of the state’s legal subjects, from whom its power flows. However, this theory is non-positivist and infused with morality. The basis of the fiduciary relationship is a legal and moral one which recognises the beneficiary’s (subject’s) dignity and capacity to place the fiduciary under obligation, just as a vulnerable ward does to a guardian, and the beneficiaries innate dignity (by virtue of its personhood) proscribes instrumentalisation – treating or regarding it as a thing (Criddle and Fox-Decent, 2009). The state must respect the agency and dignity of its subjects, and subjects (understood as those subject to its irresistible power) can be both citizens and strangers. Fox-Decent (2011, p.109) argues, in the case of non-subjects vulnerable to a foreign state’s power, that “[t]he state’s power remains irresistible and administrative in nature, and strangers too have an innate right of humanity capable of placing the state under obligation” and that “[a]rguably, our innate right of humanity alone requires the state to act subject to fiduciary constraints regardless of whether we are citizens or strangers”.

The state which exercises power over strangers does not do so with the authority of the law of these strangers’ land, and might be said to be in a position of de facto sovereignty over these strangers – its authority does not flow from them. A fiduciary relationship is still triggered when the state uses this irresistible power, and to the extent that this power is exerted, the state should be subject to commensurate constraints. The state wielding its powers extra-territorially is morally prohibited from instrumentalising or dominating its subjects on the basis that these strangers, like its own citizens, have dignity on the basis of their humanity, and agency, which must be respected. The state cannot rule on the behalf of these strangers as their sovereign; however, it has a minimal duty of negative obligations – that is, to respect the rights of the stranger (Criddle, 2014). Maximally, where the state occupies and wields complete control over strangers, the state
may have positive obligations to ensure human rights during a transition to the de jure sovereign (Criddle, 2013). Unpacking the issue of jurisdiction under fiduciary theory suggests that the *gestalt* or relational approach, rather than exclusively the protective or narrow approach, is the natural outcome.

King (2009) offers a useful tripartite model of jurisdiction consistent with the gestalt approach that appreciates the fiduciary relationship between legal subjects and general subjects (or strangers). King (2009) argues for three categories of jurisdiction, each with different packages of responsibilities:

- territorial-based jurisdiction
- jurisdiction based on non-territorial factors
- jurisdiction based on a factual relationship.

In the case of *territorial jurisdiction*, persons who fall within the lawful jurisdiction of the state (that is, those within the national borders of the state where it at least exercises full control) are owed the full range of human rights from the state, both positive and negative obligations. States may occupy foreign territories, and where this is so their authority flows from international law rather than the law of the foreign territory (Criddle, 2013). The authority is lawful but remains de facto, the state is not a sovereign but a caretaker, as argued by Criddle (2013, p.13):

> …international law entrusts the occupier, like an international trustee or mandatory power, with a guardianship responsibility to establish basic security and safeguard human rights for the benefit of those within occupied territory, including both its own forces and the local population. Thus, principles of trust and fidelity lie at the heart of the international law of occupation—despite the fact that there may be little actual trust, and perhaps even deep-seated enmity, between the occupier and the populace of an occupied territory. As with the mandate and trustee systems, a state that governs territory under belligerent occupation serves as a temporary ‘guardian’ or ‘trustee’ and bears corresponding duties of loyalty and care to the people under occupation.

The state’s human rights obligations in this situation are circumscribed by legal competence and extent of factual control, that is, human rights obligations are discharged in accordance with local law to the extent that that law is compatible with a regime of secure and equal freedom and to the extent that the occupying state has in its power to discharge its human rights obligations, for its control over the territory may be tenuous (Criddle, 2013; King, 2009).

In the case of *jurisdiction based on territorial factors* a state has ‘lawful competence based on non-territorial factors’, [King, (2009), p.548]. The state’s human rights obligations are proportional to the extent of this legal competence (King, 2009). Persons within this category would include the state’s nationals abroad, and the state’s capacity to discharge its obligations is circumscribed by the local laws of the location of that national (King, 2009). The state in this instance still holds discretionary, administrative power over its citizen [to whom it may have to issue a passport to ensure freedom of movement, for instance (King, 2009)] – though its power is limited and it is not in a position to ensure and respect all of its national’s human rights.

In the third category, jurisdiction based on a factual relationship, “…when a state, through its agents, acts beyond its lawful competence, it brings any person affected by its acts within its ‘jurisdiction’ for the purposes of the ICCPR and ECHR” [King, (2009),...
p.551]. By this approach, the state owes human rights obligations proportionate to the control exercised over the individual, though King (2009) notes, with the exception of cases of physical custody, these obligations will more often be negative in nature. Therefore the state as fiduciary, acting outside of its lawful authority, is still required to respect that rights of the distant stranger subject to its power. The innate morality of the fiduciary relationship places the state under obligation to respect the dignity of all those subject to its power, and it must act in the best interests of all subjects, commensurate with the extent of the power it wields over them. Though the state may be acting without lawful authority, this factual relationship must ultimately be viewed as being a legal one subject to legal principles. The fiduciary relationship is triggered when the state exercises power over the stranger and this relationship must be moderated by human rights.

Relying on the fiduciary theory in conjunction with King’s tri-partite typology on extra-territorial jurisdiction has offered some clarity and coherence on the extra-territorial human rights responsibilities of states, indicating a gestalt approach between the narrow and protective views; ultimately the state’s human rights obligations are commensurate with its degree of control over individuals subject to its power. This approach closes the extra-territorial lacuna.

Now, the puzzle of a state’s extra-territorial responsibility to protect the right to privacy can be explored.

7 Extra-territorial respect for the right to privacy

Before proceeding further it is appropriate to ask what the relationship is between the state and ‘stranger’ data subject, is the state acting with lawful authority or is the relationship purely factual? The state hosting, receiving or intercepting data has no legal authority over the data subject, who is a non-national living abroad in a territory where the state exercises no control. Its acquisition, storage and use of this data subject’s information is likely an exclusively factual relationship where, prima facie, the data-receiving state holds only negative obligations not to unduly interfere with the data subject’s right to privacy.

The state must comply with the established requirements of any interference with data subject’s right – that is the limitation is still subject to conditions of necessity, proportionality and the provision of safeguards from abuse. With respect for the dignity and autonomy of the subject and in order to mitigate states of domination or instrumentalisation, it must comply with basic principles of at least consent and correction where applicable. The state therefore must be open to receiving communications with the data subject and queries regarding the data held, at least to the extent that this would not jeopardise the legitimate purpose being pursued in the limitation, or where the data has not been destroyed or has been anonymised.

Though prima facie the state-recipient of the ‘stranger’s’ data holds only negative obligations to respect privacy, the current landscape of digital communications requires more. The relationship between state and stranger may be limited but not necessarily tenuous; in a world of informational de-territorialisation the state may in actuality have the capacity to do more than respect the right to privacy, but in fact ensure it too, therefore positive obligations are implied.

This article has been primarily concerned with the use of personal data in possession of state agents specifically, however there is an additional layer of complexity warranting
Information without borders

States across the world host private enterprises that hold data on individuals, and infrastructure that carries their communications. In the case of some of these enterprises, such as Facebook, the data subject voluntarily yields some privacy and allows their data to be stored and used within the norms of the context of social media. The states that host such enterprises have positive duties to provide conditions that support the right to privacy of the data subject, regardless of their territorial location – they are responsible for ensuring the contextual integrity of their information. Additionally, the ontological theory of privacy endorses the position that our data constitutes our being, by virtue of having intrinsic aspects of ourselves stored and duplicated across the world, to some extent a part of us exists simultaneously across borders, entering numerous jurisdictions – each state in possession of this information is therefore charged with a special responsibility to protect our information and not to exploit it or allow it to be exploited, consistent with the fiduciary obligation of providing conditions of non-instrumentalisation and non-domination; for privacy lost can at an extreme place us at the whims of private actors as we become vulnerable to informational harm or exploitation for profit. States have the capacity, and therefore responsibility, to discharge both positive and negative human rights obligations.

In times of emergency, treaty obligations on the right to privacy can be derogated in whole, leaving persons acutely vulnerable to rights abuse. Normless situations may arise where contextual integrity is impinged and the autonomy of data subjects severely challenged in the interests of national security or public safety. Even in such situations, where norms are overshadowed by the exception, legal principles remain in place to protect the rights of data subjects regardless of location – there must be accountability mechanisms in place and norm subversive measures open to challenge. Returning to Floridi’s theory, the indiscriminate abuse of our personal information is an abuse against our personality – violations of the right to privacy are prohibited in both normal times and emergency regardless of derogation, for instrumentalisation of our data becomes instrumentalisation of ourselves, which is strictly forbidden in the fiduciary relationship. Fundamentally, the state must preserve an acceptable level of ontological friction and by enforcing norms that protect the appropriate flow of information and empower data subjects to the most reasonable degree in light of the specific context. Interferences with privacy do not per se represent an inappropriate flow of information; however, any such interferences that reduce ontological friction and challenge the autonomy of data subjects must be subject to adequate safeguards and serve a necessary purpose.

In the informationally de-territorialised world, the protection of privacy has become a shared responsibility between states, whose physical borders are slowly diminishing in relevance. In his chapter in the book, *Fiduciary Duty and the Atmospheric Trust*, on the right to a healthy environment, Fox-Decent (2012, p.254) argues that “…every state is under a cosmopolitan *erga omnes* obligation to respect the right of the world’s inhabitants to a healthy environment”, on the basis that environmental policies in one state invariably have a reverberating effect across the world, exposing persons across the world to the consequences of state power and creating a factual relationship, essentially between all states and persons. According to Fox-Decent, “…the world’s states are joint trustees of the atmosphere, while the inhabitants of earth are their beneficiaries” [Fox-Decent, (2012), p.254]. ‘Cyberspace’ may not be ethereal when the physical infrastructure that facilitates it is fragmented all over the world, however in some sense the *res communis* comparison holds – it is a digital environment that represents a
confluence between peoples and states, and where the implications of state policy have reverberating global effects and ripple throughout networks of people. Arguably the most useful way of viewing ‘cyberspace’ is by viewing it as a res communis, a digital environment that is common to (much of) humankind, with states as the joint trustees of this digital environment, and with the respect for the right to privacy, one of those most vulnerable to abuse in this milieu, as an erga omnes obligation arising from this joint trusteeship.

8 Conclusions

This article was motivated by a desire to examine the applicability of the right to privacy in a world of constant, borderless data flows where issues of territorial jurisdiction arguably remain unresolved. It began by examining ethical theories of privacy that describe it as a condition and a right and argued that persons are entitled to appropriate flows of information protected by contextual norms, that they require a degree of control over this flow of information and that violations of privacy are aggressions against their personality.

Following this, fiduciary theory was outlined, which endorses the view that states are Fiduciaries of their people duty-bound to provide a regime of secure and equal freedom, with human rights as the blueprints of this regime.

ECtHR case law regarding privacy was briefly examined in order to demonstrate precedents set by the court defining the extent of the right and its limitations. It was demonstrated that the right is subject to interference on the basis of necessity and legitimate purpose, and so long as safeguards from abuse were present.

The contentious puzzle of extra-territorial jurisdiction was unpacked and addressed with the aid of fiduciary theory and King’s tripartite model, and it was argued that state’s extra-territorial human rights obligations were commensurate with their degree of control over individuals outside of their territory. In concluding this, the protective view and narrow view of extra-territorial human rights obligations were both rejected for a gestalt model.

In examining the right to privacy under the tripartite model, it was argued that states establish a factual relationship with an individual upon acquisition of their personal data and owe this individual negative obligations at a minimum and any interferences should be on the basis of necessity, legitimate purpose, and there should be safeguards from abuse – regardless of the individual’s location. Furthermore, it was argued that the state has a positive obligation to establish conditions that protect the right to privacy for all data subjects within the state’s jurisdiction, to the extent that the state is capable of this.

Acknowledgements

The author gratefully acknowledges Dr. Damian Jackson for his review of the manuscript and the insightful feedback offered.

The research leading to these results has received funding from the European community’s Seventh Framework Programme under grant agreement No. 607691 (SLANDAIL).
The materials presented and views expressed here are the responsibility of the author(s) only. The EU Commission takes no responsibility for any use made of the information set out.

References


Notes

1 A term coined by Luciano Floridi, it does not describe when people live but rather how they live – in this case in societies that produce and depend on digital ICTs and the abundant information they generate. See Floridi (2014).

2 As noted by Floridi (2014, p.4), at least 70% of gross domestic product of members of the G7 group (Canada, France, Germany, Italy, Japan, the UK and the USA) is dependent on information-related goods (qualifying them as hyperhistorical societies).

3 Of communications and data-flows.


5 See Big Brother Watch and Others v. the United Kingdom, 58170/13, 9 January 2014 and Bureau of Investigative Journalism and Alice Ross v. the United Kingdom, 62322/14, 5 January 2015.

6 The USA, for example, holds that it has no extra-territorial obligations under human rights treaties (van Schaak, 2014).

7 Lawless v. Ireland, 332/57, 14 November 1960.

Information without borders


10 Bernh Larsen Holding AS and Others v. Norway, 24117/08, 8 July 2013.

11 Bernh Larsen Holding AS and Others v. Norway, 24117/08, 8 July 2013, par. 174.

12 Uzun v. Germany, 35623/05, 2 December 2015.

13 Roman Zakharov v. Russia, 47143/06, 4 December 2015

14 Peck v. the United Kingdom, 44647/98, 28 January 2003

15 Leander v. Sweden, 9248/81, 26 March 1987

16 M.M. v. the United Kingdom, 24029/07, 13 November 2012

17 Khelili v. Switzerland, 16188/07, 18 October 2011


20 Weber and Sarvia v. Germany, 5934/00, 29 June 2006, par. 66.

21 Loizidou v. Turkey, 15318/89, 18 December 1996.

22 See Manitaras v. Turkey, 54591/00, 8 June 2008 and Cyprus v. Turkey, 25781/94, 12 May 2014.


