International Review of Law, Computers & Technology

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/cirl20

# The ecosystem concept: a holistic approach to privacy protection

Lauren E. Elrick

**To cite this article:** Lauren E. Elrick (2020): The ecosystem concept: a holistic approach to privacy protection, International Review of Law, Computers & Technology, DOI: 10.1080/13600869.2020.1784564

**To link to this article:** https://doi.org/10.1080/13600869.2020.1784564



Published online: 24 Jun 2020.

INTERNATIONAL REVIEW OF LAW, COMPUTERS & TECHNOLOGY
https://doi.org/10.1080/13600869.2020.1784564



# The ecosystem concept: a holistic approach to privacy protection

Lauren E. Elrick [a,b]

[a]Department of Transboundary Legal Studies, Faculty of Law, University of Groningen, Groningen, Netherlands; [b]"Mihai Viteazul" National Intelligence Academy, Bucharest, Romania

**ABSTRACT**

Proportionality remains a vague concept, in part due to the inherent difficulty of balancing two fundamentally important, but potentially conflicting values, particularly when no recognised method exists to definitively determine where the balance should lie. In the current global climate, privacy has increasingly found itself balanced against the necessity of a wide range of intrusive technological measures judged essential to the state's fight against terrorism. The range of measures involved can make assessing proportionality complicated, as relying on the proportionality test which isolates and examines a particular legal measure independently, might not adequately identify the total risk presented to an individual's privacy. In this article, it is proposed that one way of addressing this issue is through turning to the biological concept of the ecosystem for guidance. This concept recognises the existence of a closely interconnected system of actors, engaged in the exchange of information and resources. In particular, it places great importance on the interconnections between the various actors, and the effects one can have on another. This article therefore considers whether this approach can be utilised in order to conduct a more holistic proportionality assessment, and whether it provides a viable method of analysis within law.

**KEYWORDS**

Privacy; proportionality; ecosystems

## Introduction

Unlike certain rights such as the right to life, the right to privacy falls within a category of rights from which derogation is possible when necessary and proportionate to do so. However, as Van Gerven (1999, 60) acknowledges, proportionality still 'remains a vague concept'. A large part of this vagueness can be attributed to the difficulty in balancing two fundamentally important, but nonetheless potentially conflicting, values – such as the right to privacy and the right to security.

**CONTACT** Lauren E. Elrick l.e.elrick@step-rug.nl Department of Transboundary Legal Studies, Faculty of Law, University of Groningen, 9712 EK, Groningen, Netherlands

This article has been republished with minor changes. These changes do not impact the academic content of the article.

In the current global climate, privacy has increasingly found itself balanced against the use of intrusive technological measures, justified on the grounds of their necessity in order to help achieve the goals of fighting terrorism and serious crime. This is an area in which the state holds a considerable margin of appreciation in determining the most appropriate measures through which to achieve these goals, with the ultimate determination as to what is necessary and proportionate left to the state authorities. It is often only when such actions are seen as being manifestly unjust that the state is overruled by the courts. However, it cannot be disputed that states are always going to seek to justify the widest range of measures possible, in order to enable them to protect the welfare of their citizens. No state is ever going to want to be the one to have to admit they missed the potential to prevent a terrorist attack because they did not have the necessary technology to do so – especially, if such a technology actually exists. Such a desire to continually expand the range of technologies available is not fundamentally wrong, however, it can make assessing the proportionality of these measures inherently difficult.

After all, while each individual measure might be justifiable and proportionate on its own merits, when looked at from a more holistic perspective, this might not be the case. Indeed, by assessing the impact the whole range of measures, taken together as representing some form of privacy-invasive system, has on the right to privacy, it might, in fact, prove that the cumulative value of these intrusions is not justifiable. Accordingly, in these situations, relying on the proportionality test, which isolates and examines a particular legal measure independently, might not adequately identify the risk that exists to an individual's privacy.

In this article, it is proposed that one way to rectify this issue could be found through turning to the biological concept of the ecosystem for guidance. This concept recognises the existence of a closely interconnected system of actors, both living and non-living, who are engaged in the exchange of information and resources. In particular, the ecosystem concept places a great importance on the interconnections that exist between the system's various actors, allowing interferences to be made as to how the actions of one can affect the behaviour of another. This article therefore considers whether this approach can be applied to the field of law, and in particular, whether it enables a more holistic approach to be taken to assessing the proportionality of limiting the right to privacy in certain instances. The paper concludes by considering whether the ecosystem concept provides a viable method of analysis, and how it can be taken forward in the future.

## The right to privacy

There are few who would dispute the necessity of a right to privacy.[1] From an early age, we are taught the importance of respecting the privacy of others, and ensuring the protection of our own. As might be expected of any notion which holds such prominence in society, the concept of privacy has a long history. Indeed, it dates back until at least the time of Aristotle, where there developed an understanding of the need to ensure the separation of the public (*polis*) and private (*oikos*) spheres of society, in order to constrain the powers of governments from interfering into areas which they should not (DeCew 2018, 9–11; Habermas 1992).

Yet, despite its prominence, privacy is a concept that does not lend itself to being easily defined (Niemietz v Germany 1992, §29; Peck v United Kingdom 2003, §57). This is, in part, due to the 'variety of meanings and expectations' which it can encompass, and which can

vary according to the situation in which it is invoked (Hiranandani 2011, 1092; DeCew 2018). A range of aspects can be recognised as falling within the scope of the protection of privacy, including but not limited to: privacy of the person; personal behaviour; personal communications; personal data; location and space; and thoughts and feelings (Milaj 2016, 121; Himma 2007, 864). This 'inherent flexibility' has the benefit of allowing the concept to be moulded to a specific situation, enabling the widest range of protection possible, but consequently, also makes it difficult to reach a 'comprehensive and determined consensus' as to its definition (Klitou 2014, 14). At the same time, the concept has also undergone a variety of changes through the years, evolving alongside societal changes to 'public opinions, ideological trends [and] available technologies' (Klitou 2014, 14; Serwin 2009, 870).

Despite this, it has been possible to identify a central core to the concept, or the right of the individual to 'control the flow of information concerning or describing or emanating from [them]' (Hiranandani 2011, 1092; DeCew 2018; Himma 2007, 864). This has been termed the right to 'information self-determination' and recognises that when personal information is involved, it is important to an individual to know who holds this information, what happens to it and who it is shared with (Hiranandani 2011, 1092; Westin 1967, 5). In this manner, privacy can be thought of as representing something like a shield, protecting the individual from the unreasonable intrusiveness of others, and enabling them to live their life in the manner of their choosing (Hiranandani 2011, 1092; Himma 2007, 864; Westin 1967, 26).

Thus, it is hard to understate the importance the right to privacy holds for the individual, not least because of the role it plays in ensuring respect for human dignity, but also through enabling individuals to have the space and freedom to identify who they are as a person, by removing them from the influence and judgement of others (Klitou 2014, 19; COE 2019, 33). Indeed, without this space through which to develop their personal identity, individuals fail to fully develop their own independent thoughts and opinions, and are consequently more likely to succumb to the pressure of society to conform with recognised ideals (Klitou 2014, 19). As such, privacy should be thought of not only as an independent right, but also as an 'enabling right', granting everyone the opportunity to exercise their 'fundamental right to the free, unhindered development of [their] personality' (UN SRP 2016, §7). It is because of this enabling ability that privacy has been recognised as being 'at the core of all basic freedoms and … the foundation from which all other human rights and freedoms flow' (Hiranandani 2011, 1092).

## Legal recognition

Despite its long history, the right to privacy was only recognised as a human right for the first time in 1948 within Article 12 of the Universal Declaration of Human Rights (UDHR). This was followed by the creation of a near identical, but binding, right within Article 17 of the International Covenant on Civil and Political Rights (ICCPR).

Within Europe, the right to privacy has been protected under Article 8 of the European Convention on Human Rights and Fundamental Freedoms (ECHR). This states that 'everyone has the right to respect for his private and family life, his home and his correspondence'. As its primary purpose, Article 8 protects the individual against arbitrary interferences into these areas by a public authority (Libert v France 2018, §44–42). This can be thought of as imposing a negative obligation on the state, similarly to that of

the ICCPR (UN SPCT 2009, §11). However, the ECHR also contains a positive obligation, requiring the state to explicitly recognise the existence of the right and ensure its respect, even between private parties (UN SRCT 2009, para 11; Bărbulescu v Romania 2017, §108–111).

The European Union (EU) also recognises the existence of the right to privacy, provided for within Article 7 of the EU Charter of Fundamental Rights (EU Charter). Notably, the EU Charter also recognises the existence of the right to data protection, as a distinct and separate right (EU Charter, Art 8) from the right to privacy. This right protects the individual from the improper use, collection, storage or sharing of their data. That the rights to privacy and data protection are considered as distinct and separate is an important facet of the EU system, as opposed to the ECHR system which incorporates the right to data protection within the right to privacy (COE 2008, 4). Thus, while Article 8 ECHR creates a general right to privacy, encompassing the protection of personal data; the EU Charter creates a *sui generis* right (COE 2008, 7).

## Qualified status

Unlike some human rights, such as the right to life, the right to privacy is not absolute, but rather can be limited in certain circumstances. In these situations, even though a violation of the right has occurred, it shall be regarded as having transpired for a legitimate reason. This relates back to the understanding that on certain occasions, there shall be a need to balance the competing interests of the individual with that of the community as a whole, for example, by interfering with an individual's right to privacy in order to protect national security (Hämäläinen v Finland 2014, §65; Gaskin v United Kingdom 1989, §42). In these situations, what is important is that a fair balance is found between the competing interests (Soering v United Kingdom 1989, §89). An interference is only permitted if it fulfils the criteria laid down within Article 8 ECHR. Accordingly, Article 8(2) ECHR declares that:

> 'there shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being 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.'

This provision thus creates three requirements that must be complied with in order to legitimately restrict the right to privacy. Failure to comply with any one of them will result in the interference being classed as unlawful and thus shall constitute a violation of the right to privacy. The first requirement is that the interference must be 'in accordance with the law', which requires that it must be laid down in domestic legislation which is accessible, foreseeable, and complies with the rule of law (Sunday Times v United Kingdom 1979, §49; Silver and Others v United Kingdom 1983, §87; Fura and Klamberg 2012, 471).

Secondly, the interference must pursue one of the listed interests provided for within Article 8(2), such as the protection of national security or public safety. The obligation lies upon the national authority to prove that any interference pursues a legitimate aim (Mozer v Republic of Moldova and Russia 2016, §194).

The third and final requirement is that it must be 'necessary in a democratic society'. In order to satisfy this requirement, it must be shown that the interference addresses a 'pressing social need', is proportionate to the aim pursued, and based on 'relevant and sufficient reasons' which are capable of justifying that particular interference (Sunday Times v United Kingdom 1979, §59; Olsson v Sweden (No.1) 1988; Dudgeon v United Kingdom 1981, §51–53). In doing so, the Court engages in a balancing exercise, pitting the interests of the member state against those of the individual.

## The principle of proportionality

The focus of this article, therefore, relates to this third and final requirement: that any interference must be 'necessary in a democratic society'. In establishing this, a balancing exercise is often required, during which the interests of the individual are contrasted with those of the wider community, in order to reach a fair balance between the two (Keegan v Ireland 1994, §49; Milaj 2016, 116).

This balancing exercise is often carried out through applying the proportionality principle. The concept of proportionality has been present in legal parlance for generations, originating from the concept of justice advocated by Aristotle in Book V of Nicomachean Ethics, which required that in order for an exchange between individuals to be considered fair, the balance of the benefits and contributions between the two must be equal (Johnston 2011, 67; Engle 2012, 10; Aristotle 2019). It now represents a generally recognised principle of law found globally, in both civil and common law sources. According to Engle, while more refined and precise, the modern conception of proportionality is still largely based on that elucidated by Aristotle centuries ago (2012, 4).

Proportionality is a useful concept, as it relies on the assumption that what is desired through decision-making is balance – that by finding the point where all things can be viewed as equal, we will be able to reach the fairest, and consequently, best decision (Tsakyrakis 2009, 469). For most people, the most familiar usage of the principle is in relation to the case law of the ECtHR.[2] Its first usage came in the Handyside case, wherein the court laid down a strict set of criteria to be applied before limiting human rights. Firstly, is there a pressing social need for the limitation? If so, does the restriction correspond to this need? Is the restriction a proportionate response, or does it overstep? And finally, have the authorities presented sufficient and relevant reasons for the necessity of the restriction? (Milaj 2016, 118; Handyside v United Kingdom 1976).

As such, it establishes the understanding that whenever a state wishes to carry out an act which has the potential to infringe rights, it must represent a 'rational means to a permissible end' in order to be acceptable – and it can only authorise an infringement to the extent necessary to achieve their goal (Engle 2012, 2; Barak 2012, 3; Z v Finland 1997, §94). Thus, the principle plays a dual role – by setting restrictions on the infringement of fundamental rights, it ensures their protection, but also recognises the existence of legitimate reasons which might require its limitation (Milaj 2016, 117).

In evaluating the proportionality of a measure, the ECtHR largely relies on analysing and assessing the legislative choices the state has made (COE 2019, 12). In doing so, they take account of the margin of appreciation afforded to the state. This concept recognises the inherent difficulty involved in balancing competing rights, and therefore works on the assumption that the state is usually the best authority for determining whether a particular

interference with a human right is necessary or not. The degree of leeway afforded to the state can be affected by a number of factors. When the interference relates to a particularly important aspect of the individual's identity or existence, the margin of appreciation will be restricted (X and Y v Netherlands 1985, §24, 27; Christine Goodwin v United Kingdom 2002, §90). Meanwhile, areas in which there is a lack of consensus between the Member States as to the importance of the interest affected or the best manner for its protection, and particularly in relation to issues sensitive to the state, result in a wider margin of appreciation (X, Y and Z v United Kingdom 1997, §44; COE 2019, 9). In particular, when it comes to striking a balance between competing private and public interests, or balancing one Convention right against another, the margin afforded to the state is considerably wide (Odièvre v France §44–49). Thus, as Serwin (2009, 876) acknowledges, the principle of proportionality ensures that those pieces of personal information which are of limited interest to others, but yet highly sensitive to an individual are protected behind a series of restrictions and barriers, while still permitting those with a legitimate need to know a right to access, particularly when relating to the less sensitive interests of the individual.

However, the act of striking a balance between two competing rights is inherently difficult. After all, in some situations it might be clear in what direction the balance should fall – very few people would argue that it was disproportionate to subject an individual suspected of planning a terror attack to temporary surveillance. However, in other situations, the decision is not so clear cut. What about the use of facial recognition technologies in public spaces? Finding a balance between two rights rests on the assumption that the two rights have a recognised weighting which enables them to be compared, and a definitive conclusion to be reached (Milaj 2016, 117; Harbo 2010). It suggests precision, that a calculation is possible, in order to determine which right outweighs the other (Tsakyrakis 2009, 469; 474–475). However, when it comes to competing human rights values, there are no rational standards which can be applied in order to balance one against another (Milaj 2016, 117; Harbo 2010). And, as is often the case, when privacy is contrasted with a right such as the right to security, the balance is often not seen to fall in privacy's favour.

## The right to security

The concept of security, much like that of privacy, does not lend itself to easy definition. In fact, it has been well recognised as representing a 'complex and contested notion' which is further complicated by the fact it is 'heavily laden with emotion and deeply held values' (Kolodziej 2005, 1; Baldwin 1997). At its most basic, security is recognised as encompassing the protection of an individual from serious threats to their wellbeing, life or livelihood. Security is therefore about the protection against threats. As Wolfers (1952, 485) describes, this contains both an objective and subjective element – objectively, it relates to the absence of threats; while subjectively, it looks at the absence of fear that a threat shall occur. As we enter a new decade, it is clear that we live in a world facing a wide range of diverse threats – the ever present menace of international terrorism; insecurity and poverty, which millions around the world still live in; the ongoing immigration crisis, which the likely re-ignition of tensions in the Middle East will only acerbate; as well as the looming threat posed by global warming. When the loss of security holds such

serious consequences, it is no wonder that there is often the tendency to suggest that the state is legitimised in using all methods possible in order to ensure the security of their citizens.

Both the terms security, and national security are highly ambiguous (Kolodziej 2005, 21). Indeed, it is their ambiguity that plays into the hands of those who, while generally holding good intentions, are most likely to exploit it. After all, the ambiguity of the term 'security' is such that it results in it being used to cover a range of values so wide as to encompass almost anything that is desired (Kolodziej 2005, 21; Wolfers 1952, 484). And, as Wæver (2011, 94–95) highlights, this has led to a process known as securitisation, whereby labelling an act with the term 'security' opens up the potential for the state to claim a special right to act out-with the scope of normal actions.

When thinking about security, it is difficult to refer to the concept without considering the work of Thomas Hobbes. After all, for Hobbes, ensuring the continued existence of peace for their citizens was the entire aim of the state (Lazarus 2015, 424). In his perception, citizens traded a portion of their liberty to the state, in return for the assurance of security (Lazarus 2015, 424; Himma 2007, 889; Hobbes 2018). This was because, all men being equal, were disagreements to occur between individuals regarding the possession of a good that was desired by more than one individual, but which could only be owned by one, there was no way of determining who was entitled to be the true benefactor (Hobbes 2018, 112–113; Lazarus 2015, 424; Kolodziej 2005, 53). As a result, the situation was likely to descend into a state of violence – or war – which would inevitably result in the denial of one of the individuals of their right to liberty, or even life (Hobbes 2018, 113). In order to avoid such a situation, citizens consented to placing unlimited power into the hands of the sovereign, in return for them ensuring the continued existence of peace and preventing the outbreak of war (Lazarus 2015, 424). A criticism of his concept however is that it did not appear to foresee that the sovereign itself could pose a threat to the security of the state (Lazarus 2015, 425).

In contrast, John Locke believed that all individuals were equal on account of their natural rights – those of the right to life, liberty and property – and that it was the responsibility of the state to ensure the enjoyment of these rights (Lazarus 2015, 425; Locke 1948). As such, the individual had a right to police and punish all those who attempted to infringe their enjoyment of these rights (Lazarus 2015, 425). As opposed to the unconditional transfer of rights to the sovereign conceptualised by Hobbes, for Locke, any transfer of rights was conditional – the power granted must be used for the individual's benefit, or they were entitled to take back the power granted to the sovereign (Lazarus 2015, 425–426). For Locke, it was important that there were constraints placed upon the power of the sovereign, achieved through the use of law, in order to ensure that citizens were not subjected to the arbitrary power of the sovereign (Lazarus 2015, 426).

Whether as an obligation of the state towards their citizens, or as a method of ensuring the enjoyment of an individual's fundamental rights, what is clear is that the principle of security is an important one. Indeed, it is regarded by many as representing the most important right that an individual is entitled to, on account of the fact that it can be considered an essential component to the enjoyment of all other rights (Shue 1996, 67; Himma 2007, 884). After all, if you do not have security, how can you possibly enjoy the existence of the other rights to which you are entitled?

## Balancing privacy with security

When considered in this manner, it becomes clear why there is an inherent difficulty in balancing the rights of privacy and security. After all, privacy guarantees an individual the ability to freely develop their personality and identity without being subjected to the wills of others, while security grants them the chance to live their life in this manner without being subjected to threats that would deny them this opportunity.

In the post 9/11 period, there has been a tendency to view the world that we live in as fundamentally changed from that which existed prior to the 2001 attacks – one which requires a new set of tools and strategies in order to combat the threats that society now faces from dangers such as terrorism (Hoffmann 2004, 949). In large part, this has stemmed from the failure of the US intelligence community to identify the threat prior to the attacks – blindsided, and determined to prevent the same thing from occurring again, there were calls for an increased reliance on methods which could predict, and thus prevent, terrorist attacks before they occur (Mitsilegas 2015, 36). Such methods increasingly relied on the collection of data, and large amounts of it. Regardless of whether you agree with the methods advanced, the intention behind them is clear – recognition of the fact that every individual is entitled to the rights to life and security, and the obligation that lies upon their government to ensure the respect and fulfilment of these rights (Hoffmann 2004, 949).

It is an unquestionable fact that there will be instances in which the right to privacy will need to give way to the right to security. Of this, there is little dispute. However, problems begin to occur when they are thought of as being intrinsically opposed to each other. When individuals talk about the need to find some balance between the two, it often presents the situation as one in which one right must automatically trump the other. As some authors, such as Schneier (2015, 155), but also Feinberg (2015, 390) argue, presenting the situation in this manner, as a trade-off between security and other human rights such as privacy, is disingenuous – it typically asks citizens to give up their right to privacy in return for security and enhanced protection, rather than suggesting that it is possible to have both. In addition, the specific risks for which citizens surrender their privacy are rarely specified, or identifiable to the average individual (Valkenburg 2015, 255), meaning it is not possible for them to engage in their own calculation (and even if they could, this assumes that it is possible for them to then remove themselves from the calculation).

Furthermore, as Chandler (2009, 112) notes, security is often envisaged as the 'trumps of trumps' – when positioned against it, there are very few rights which it could be said to outweigh it. As some authors such as Himma (2007, 872–873) assert, all things being equal, security should always be thought of as more important than privacy. As he sees it, while both privacy and security represent moral values worthy of protection in our societies, they should also be thought of as in a hierarchy. And security falls at the very top of that hierarchy.

Of course, the objection to this point of view is that very rarely are we comparing equal values. Often it is not clear what the actual results of any particular security measure are, and moreover, it is nearly impossible to put a value on the costs occurred as a result of the loss to an individual's right to privacy. Indeed, as Tsakyrakis (2009, 474–475) emphasises, when we talk of balancing it carries the 'connotations of mathematical precision' – something that is impossible to determine when balancing privacy and security. The gains from

any specific security measure are unquantifiable, as rather than resulting in an increase in security, what they actually achieve is a decrease in the risk that something might occur in the future (Moeckli 2008, 9). And as Moeckli (2008, 9) emphasises, when we think of risk, we do not think about it rationally – particularly when dealing with emotive topics such as terrorism. Consequently, when the protection of security, and particularly the prevention of terrorism, is placed on one side of a balancing scale, it is frequently thought of weighing more than it probably should.

The result is that proper discussions as to how to balance rights such as privacy and security do not take place – rather, when posed against security, there is a tendency to assume the inferiority of the other right – that if it is claimed it is necessary to restrict it, then it must be so. After all, a lack of security can result in fatal consequences, while privacy is only a loss of information. When posited in this manner, it seems irresponsible to contest that security could be trumped by another right such as privacy. However, this failure to properly engage in a fair scrutiny of the competing interests of the two rights means that important questions such as whether the measure actually does increase security like it is claimed; whether there are less privacy-invasive methods of achieving the same goals; whether the gains to security are worth the cost of the loss of privacy; and whether there is a fair distribution of the costs, or whether they are unfairly borne by a minority group in order to increase the security of the majority (Chandler 2009, 122), do not get answered. And, as Hoffmann (2004, 934) muses 'history shows that when societies trade human rights for security, most often they get neither'.

Indeed, as the current UN Special Rapporteur on the Right to Privacy states, as opposed to thinking in terms of privacy versus security, what we should be talking of is privacy and security (2016, §23). Both are fundamental values upon which our society rests. As such, rather than talking of human rights in opposition to security, what we should be looking for is what Feinberg (2015, 391) describes as a 'healthy combination'. Indeed, an examination of the case law of the ECtHR shows a desire to achieve this. Thus, for example, even in regards to the prevention of terrorism, where a well-recognised justification for the limitation of privacy exists (Segerstedt-Wiberg and Others v Sweden 2006, §88), there are still limits to what is justifiable. As noted in S and Marper v United Kingdom (2008), despite arguments of its 'inestimable value in the fight against crime and terrorism' (§91), the Court was unwilling to accept the limitless retention and use of DNA samples, as to do so would 'unacceptably weaken' (§112) the protections afforded by Article 8. Instead, they urged for a careful balancing of the benefits of such technologies with the private life interests of the individual (§112). Likewise, where automatic processing techniques are applied to personal data, greater safeguards are required in order to ensure that solely relevant data is used, and only to a justifiable extent (Gardel v France 2009, §62). Such a requirement is necessary in order to prevent unjustifiable interferences into the right to privacy.

Similarly, the CJEU has also laid down requirements for the balancing of privacy interests with the achievement of security related goals.[3] Take, for example, *Digital Rights Ireland* (2014), in which the Court noted that while the prevention of terrorism was of general interest (§42), and the collection of electronic communications data was a valuable tool in achieving this goal (§43; 51), its retention must still comply with the rules of proportionality. Thus, on account of the pervasive effects that this form of data could have on an individual's privacy, and the indiscriminate and generalised nature of its collection,

the Court found that, *in this manner*, its retention did not comply with the recognised principle of proportionality, and accordingly invalidated the Data Retention Directive (2006/24/EC). The Court subsequently reaffirmed the illegitimacy of legislation sanctioning indiscriminate and generalised schemes of data retention, even on the grounds of fighting serious crime and terrorism, in the case of *Tele 2 Sverige and Watson* (2016, §112).

What these cases highlight is that both the ECtHR and CJEU are willing, and able, to balance the rights of privacy and security, and determine that the privacy interests of an individual should come out on top of potential security gains, when necessary to do so. However, each of these cases only examines the effect that a particular measure, when considered in isolation, has on the right to privacy. In this manner, the judgements of the Courts display a form of tunnel vision, failing to appreciate the wider effects that a range of privacy interferences might have on an individual's rights.

## The ecosystem: inspiration for a holistic approach to privacy protection

How can this situation be resolved? The answer is by encouraging the development of a more holistic approach to assessing the proportionality of infringements into the right to privacy. As emphasised by Kaiser (2018, 546), a weakness of the current systems for protecting privacy is that they are 'limited to examining one law at a time'. This has the effect of narrowing the level of protection afforded to the right, on account of the fact that in the modern era, the rights to privacy and data protection are now being subjected to an onslaught of attacks from an unprecedented, and ever increasing, range of infringements – from both public and private sources (Kaiser 2018, 546). In particular, the growing range of measures now in operation in Europe, as well as a lack of transparency and accountability regarding what is collected, and for what purposes, means that it is almost impossible for individuals to effectively ensure the protection of their fundamental rights (Kaiser 2018, 546–547). Indeed, the high number of interferences mean that it would be impossible for the individual to identify each possible method through which their privacy could be interfered with, and then assess whether it was proportionate or not (Kaiser 2018, 546–547).

The situation is further complicated by the fact that while examined individually, interferences might not be classed as disproportionate, but when added together cumulatively they might amount to a violation. Indeed, as the system currently operates, the Courts are bound to study the legislation in isolation, and even then, only upon challenge from an individual (Kaiser 2018, 547). As Kaiser (2018, 555) sees it, this 'absence of meaningful standards against the cumulative effect of intrusions into the right to privacy should be regarded as a grave threat to the fundamental rights of the individual'. I can only agree with this assessment.

One way in which this unsatisfactory situation could be addressed is through the application of a holistic approach. Such an approach has been supported through the case law of the German Constitutional Court,[4] as well as Opinion 01/2014 of the Article 29 Working Party, which stated that:

> "Particularly after 9/11 the European legislator(s) have been extremely active adopting new measures limiting the rights to privacy and data protection in the [Area of Freedom, Security and Justice]. This development makes it particularly important to take a holistic viewpoint when assessing the interference with privacy and data protection of a new legislative proposal. In order to say whether a new legislative proposal is still proportionate, it is necessary to

> assess how the new measure would add to the existing ones and whether all of them taken together would still proportionately limit the fundamental rights of data protection and privacy." (2014, 21)

However, as Kaiser highlights this is easier said than done, as a method would need to be established in order to carry out this holistic assessment. It is my suggestion that one way of doing this would be to apply the ecosystem concept as a method through which the potential consequences for privacy of a new piece of legislation could be assessed. Proportionality is a difficult assessment to conduct on account of the fact that balancing competing rights without being able to properly assess their value in relation to each other results in ambiguous and questionable results. However, the concept of an ecosystem provides a method through which to identify all of the various actors present in any given situation, to understand how they are interconnected and interact with each other, and thus to determine the various effects that any particular action might have on these relationships. In applying such a concept to any measure limiting the right to privacy, it requires that a proper balancing of all of the various factors be conducted and thus enables a better determination to be made regarding the possible consequences for privacy.

## The ecosystem concept

The ecosystem concept has primarily developed within the fields of biology, and specifically ecology. For the purpose of this article, the usage of the term ecosystem shall be taken to reflect that as has been used within the field of ecology. That being said, despite its origins within the biological sciences, in recent years a wide range of fields have turned to the term ecosystem for inspiration.

One method which is seen frequently is utilising the term ecosystem as a way of highlighting the existence of connections between a variety of actors in a particular field, such as in reference to a business ecosystem, or a social media ecosystem. Such usage, however, represents a quite shallow reliance on the term – it recognises the mutual relationships between a variety of actors, however, it fails to take account of any of the intricate features of the ecosystem which can also prove beneficial for analysis. Other usages, such as that by Woolley (2014, 2020 ), have relied on the term in its ecological context, in order to provide guidance on how to develop areas of law, such as environmental law. In this manner, Woolley considers how the law can be utilised in order to protect natural ecosystems, looking at the intricacies of the natural ecosystem and what this means for law and policy makers. Finally, others such as Mars and Bronstein (2018), Norris and Suomela (2017) and Pickett and Cadenasso (2002), have considered the potential benefits and pitfalls of utilising the ecosystem concept as a metaphor within other fields of research, in particular highlighting how its flexibility makes it beneficial to a wide range of actors (Pickett and Cadenasso 2002, 6); but, also recognising that the ability of humans to engage in rational decision-making may affect 'man-made' ecosystems in ways in which a natural ecosystem would not be, and that this should be recognised (Norris and Suomela 2017).

This article has taken all of these usages into account, and considers an alternative approach – using the ecosystem as a model through which the law can consider how to appropriately balance competing interests, particularly where a variety of actors are involved, and who might be intricately linked to one another.

The concept of the ecosystem was first introduced to ecology by the English botanist Sir Arthur Tansley in his seminal work, *The Use and Abuse of Vegetational Terms and Concepts*, published in 1935.[5] Prior to the introduction of Tansley's concept, ecology – or the scientific field of study that analyses the interrelations taking place among and between organisms; and between them and their physical surroundings (known as the *environment*) – focused heavily on the interactions that took place only between living organisms, in determining how they came to live together (Van der Valk 2014, 296; Golley 1993, 24). This view was shared by Frederic E. Clements, an American botanist, considered one of the most prominent ecologists of the late nineteenth and early twentieth centuries, and a pioneer in the area of vegetational succession – Tansley himself designated Clements as 'by far the greatest individual creator of the modern science of vegetation' (Tansley 1935, 285). According to Clements, ecological communities (the group of two or more species of organisms which can be found living in the same geographical location at a particular point in time) were in a constant state of evolution (Willis 1997, 268). In particular, he believed that through a continuous series of adjustments to the relationships between the various organisms, the ecological community developed until it reached its 'optimal state', otherwise known as the *climax community* (Clements 1916; Odum 1971).

Clements believed that simple stimulus-response interactions between the physical environment and the plants present, such as a change in the environment (the stimulus) prompting a reaction from the organisms (the response), were responsible for the particular manner in which plants came to be distributed (Van der Valk 2014, 295). As such, he believed that the ecological community was formed as a result of how the environment surrounding it operated, and the resulting reaction this caused the community to have in response to the environment (McIntosh 1985, 194). Above all else, it was the particular combination of the community members that was influential in determining how it changed and adapted (Pickett and Grove 2009, 1).

As this quote from Golley (1993, 24) highlights:

> 'In most community studies and especially in the Clementsian theory of succession, the focus was on the biota and the biotic interactions and processes thought to control community dynamics. The environment was considered to be a secondary factor; frequently, it was called a stage on which the biota acted a drama.'

Clements' community concept remained the primary explanation for several decades, however, it was by no means universally accepted, or without detractors (McIntosh 1998, 427; Pickett and Grove 2009, 2; Gleason 1917). However, the most well-known criticism of Clements' ideas came from Arthur G Tansley in the form of his ecosystem concept. In particular, Tansley was critical of Clements' stimulus-response conception, feeling that it oversimplifies the 'complex relationships between plants and the environment' (Van der Valk 2014, 296; Blackman and Tansley 1905).

So large was Tansley's disagreement with Clements' thinking on this matter that he felt compelled to present his own notion in opposition. He defined it as 'the whole system (in the sense of physics), including not only the organism-complex, but also the whole complex of physical factors in the widest sense' (Tansley 1935, 299). As he acknowledged, while 'organisms may claim our primary interest, when we think fundamentally we cannot separate them from their special environment, with which they form one physical system' (Tansley 1935, 299).

The inspiration behind the ecosystem concept came from Tansley's desire to apply the notion of systems, which had gained prominence in the fields of physics and engineering throughout the course of the twenty-first century, to the field of ecology.[6] The name itself, *ecosystem*, derives from the combination of the two terms. It has been suggested that the inspiration behind Tansley's decision to use the notion of 'mentally isolated systems' as the fundamental unit within his concept of ecology came from H Levy's 'The Universe of Science' (1932; Van der Valk 2014, 316). In it, Levy highlights the reasoning behind the need to identify isolated systems, and positions this need within the field of scientific research: 'science, like common sense, sets out in the first instance to search for systems that can be imagined as isolated from their setting in the universe without appreciably disturbing their structure and the process they present' (Levy 1932, 45). Tansley was highly convinced by this idea of isolating systems in order to facilitate their better examination (Tansley 1935, 299–300). He was particularly keen to emphasise, however, that there was a certain artificialness to these isolations – as in practice these systems are not separate and distinct, but can also be included within other larger systems as a constituent part, or can 'overlap, interlock and interact' with other systems (Tansley 1935, 299–300).

According to Tansley, these ecosystems should be thought of as representing the 'basic units of nature' (Tansley 1935, 299). Unlike Clements, Tansley thought that when analysing ecological communities, the method used should include not only the living elements, such as the organisms present, but also the non-living elements, such as the environment, which had previously been largely disregarded. As he reasoned,

> our natural human prejudices force us to consider the organisms … as the most important part of these systems, but certainly the inorganic 'factors' are also parts – there could be no system without them, and there is constant interchange of the most various kinds within them, not only between organisms but between the organic and the inorganic. (Tansley 1935, 299)

Thus, when studying how and why an ecological community exists as it does, understanding the interactions taking place between the living and non-living elements, and how they operate together in order to form a stable system is an essential component (Russell et al. 2006, 113). Consequently, both the living and non-living elements should be thought of as being 'integral part[s] of a single system' (Platjouw 2016, §1.4.1).

These interconnections are numerous and play a fundamental role in the functioning of the system, to such an extent that it is impossible to isolate and analyse a single element independently (Platjouw 2016, §3.1). Indeed, the behaviour of the various elements is so connected to that of those to which it is linked, that to separate them for analysis would only result in flawed conclusions, and in no way reflect the actual functioning of the ecosystem. For that reason, the system must be understood for what it is, a system. The connections between the various elements are an integral part that should not be overlooked. Indeed, while these systems generally comprise of a considerable number of diverse parts, it is the interactions between them that result in the formation of the unique patterns which can only be attributed to that particular system (Platjouw 2016, §3.1).

Consequently, while the precise make-up of the different actors in the ecosystem is important, it is the interconnections between them which defines why the ecosystem works in the manner that it does. This is an undeniable facet of the ecosystem, on

account of the fact that the system works as a whole, and not simply as a collection of individual parts. It is not possible – nor should it be considered a valid exercise – to simply consider the actions of the components individually. In order to understand why a particular ecosystem works in the manner that it does, they have to be considered together. The importance of these interconnections can be exemplified through the fact that should a change occur to any one of the actors in the system, it can result in subsequent consequences for other actors all throughout the system – such is the intrinsic interconnections between them (Platjouw 2016, §3.1.4).

It is, therefore, clear that the interconnections between the different actors of the ecosystem are one of the most fundamental points of the concept. If you do not understand how the different actors are connected, how they relate to one another, and how one actor can influence another, it is impossible to understand how the system operates as a whole. To focus on one actor alone, rather than the whole spectrum of diversity present in the system, means that you will fail to understand why it operates in the manner that it does.

## Applying the ecosystem concept

The question, therefore, is what benefit might this concept of the ecosystem have for privacy? The answer is by encouraging the development of a more holistic approach to accessing the proportionality of infringements into the right to privacy.

### *(1) Interconnections*

One reason why the ecosystem is particularly suitable for this purpose is its emphasis on the issue of interconnections. As previously highlighted, it is only through understanding how the various actors are connected to each other that it is possible to understand how the ecosystem works in practice. A similar concept could be applied to privacy infringements – for example, whenever a new piece of legislation is proposed, it could be required that all of the potential actors who could be affected by, or affect others, on the basis of that piece of legislation should be identified (e.g. state governments, international institutions, national bodies), coming up with an 'ecosystem' for that particular piece of legislation.

This could then be compared and contrasted with the ecosystems for already existing pieces of legislation, in order to see whether there are any areas of overlap which might lead to potentially disproportionate effects on an individual's right to privacy. In this manner, the ecosystem concept could be utilised as a mapping tool, allowing the whole picture of the potential effects on privacy to be identified. Once all of the actors have been identified, it is then possible to understand the effect that one actor might have on another. Identifying the range of actors present is a valuable exercise, as it soon becomes clear how interlinked they are, and the range of consequences this can hold for privacy.

### *(2) Interactions*

Another useful feature from the ecosystem concept comes from the recognition of the interactions taking place between the various actors. In this manner, while it is vital to

identify how the various elements are interconnected, it is equally important to consider the effect that these connections can have on other actors in the system. In particular, it should be considered which actors might have a disproportionate effect on others – the keystone actors, if you will – or be disproportionately affected (e.g. vulnerable groups such as minorities) by the ecosystem. In this regard, it will be important to see whether particular actors are repeatedly subjected to interferences with their rights, and whether this can be justified when looked at cumulatively.

In biological ecosystems, it is through the interactions that the various actors share information and resources. As such, in our privacy ecosystem, it will also be important to consider how the various actors share and store the information they collect. Do they hold it for their personal use only? Is it transferred to others? How do they ensure its continued protection once it has been transferred to another actor? In addition, under which justification has the transfer of data been authorised? These are important issues which are not considered when looking at the proportionality of the collection of personal information, yet could have important consequences for determining the extent of an interference to an individual's right to privacy. With every passing second, the amount of data collected grows, a not insignificant amount of which relates to personal data. The more and more data is collected, and the greater the number of actors who have access to it, the higher the risks are from any potential leak of this data – particularly when information is held by private actors, who are not subjected to the same standards as state authorities are. After all, while you can change a credit card, or have a new ID issued, you cannot change your fingerprints.

### *(3) The non-living element – technology*

This final section focuses on the growing presence of technology in our modern societies. As Tansley forecast all those decades ago, our natural human tendencies tend to cause us to focus on the living elements of our system (1935, 299). We look at how new pieces of legislation are required in order to protect people – how they can keep us safe and secure. We anticipate the benefits that they can bring, the people they can potentially save. Especially when relating to the issue of protecting security, there is a tendency to consider that any method that can produce a quicker, more accurate, less humanly fallible result is to be seized as soon as possible.

In recent years the use of digital technologies has expanded exponentially, in a manner that few could have anticipated. In 2013, it was estimated that around 4 zettabytes of data ($4 \times 10^{21}$ bytes) had been created (Agnellutti 2014, 2). By 2018, this had risen to 33 zettabytes, and by 2025, it is predicted to reach 175 zettabytes (Coughlin 2018). As Agnellutti outlines, one zettabyte equates to every single American taking a digital photograph every single second, of every single day, for over a month (2014, 2). This is a tremendous quantity of data, which has come to characterise what has become known as the 'big data' era. The term big data is colloquially used to refer to the existence of what is known as the 3V's of data – *volume, variety and velocity* (Broeders et al. 2017, 310). Volume acknowledges the existence of large quantities of data, variety refers to the existence of the diverse range of sources from which the data originates, while velocity recognises the rapid speed at which this data can be collected and processed (Broeders et al. 2017, 310). This rise in the use of big data has had significant consequences for the manner in which personal

information can be collected, stored and processed. With this increased availability has come an increased desire to process and analyse this information to its fullest extent – if there is a way in which this information can be used in order to protect security, then those in positions of authority wish to access it. The fact that the information is readily available is increasingly seen as an incitement to use it.

However, there is often a tendency to discount the effects that technology can have on human rights, or the unintentional results that can occur. Take for example the use of algorithmic technologies, which is only growing and diversifying as time passes. On more than one occasion, when such a technology has been utilised it has resulted in either (a) unexpected or unanticipated results or (b) manifestly incorrect ones.[7] However, the explanation often given is that 'the algorithm did it' – the responsibility and blame passed along to others.

Writing back in 1991, Bennett eloquently articulated the threat that technology can play to the right to privacy. As he stated, technology

> 'is not simply a tool, but a complex set of social relations, continually being adapted and refined. The problems associated with the computer stem from the complex interdependence between people, equipment and techniques, which only together constitute information technology'. (64–65)

In our privacy ecosystem, it is posited that the place of the non-living element should be filled with technology. In this digital era that we live, the presence of technology within our lives is inescapable. Digital technologies enable us to communicate with individuals all over the world, in real time. They allow us to search for, and consume information, at a far higher rate than ever before. They have sped up processes, finding quicker methods of completing tasks that previously would have been time-consuming and costly activities. But, just as these features can be used for good, they can also be used to harm others.

Consequently, for those who are tasked with keeping us safe, such as law enforcement and intelligence agencies, these technologies play an important dual role – as (1) a source of information, for example through internet surveillance (Brown 2009) or social media analysis (Scassa 2017), and (2) by providing new methods through which they can conduct their tasks, for example, using facial recognition technology to search through large groups of individuals for people of interest (European Union Agency for Fundamental Rights 2019).

However, the use of these technologies can pose significant risks to our human rights, such as the right to privacy. Accordingly, it is proposed that within our privacy ecosystem, whenever a new piece of legislation lays down technological requirements, or suggests that a new piece of technology, such as facial recognition software, should be used in order to protect security, these must also be considered in light of the effects that they could have on the right to privacy. They should be thought of not in isolation, but in addition, to those technologies which are already used. For example, if CCTV is already widely used within an area, how would it affect an individual's privacy if facial recognition technology was added to this? This way even technologies which are not strictly governed by legislation, or not yet covered by any law, but yet might still have an effect on an individual's privacy could also be included in the system.

The increasing presence of technology has also generated another important aspect which needs to be considered within the proposed ecosystem. As the range of

technologies which are seen as beneficial widens, it creates a growing reliance on the private sector. Most of the technologies utilised by law enforcement and intelligence agencies are developed not by states, but rather through private innovation (Brown 2019, 1). This brings a new dimension into the ecosystem, as it no longer includes only the individual and the state, but also the private sector, which might not even be based in the same country as the individual. This can raise particular concerns for privacy, as while states are required to respect human rights, there is no such binding obligation on the companies which create these technologies (Couzigou 2019, 18). As the presence of new technologies within our daily lives only continues to grow, this will have important implications for our human rights – by providing a method through which to catalogue the various risks, the ecosystem concept could offer a method of ensuring their protection.

## Conclusion

When analysed through the lens of the proportionality principle, the right to privacy often finds itself balanced against other important rights such as the right to security. In the process of this balancing exercise, infringements with the right to privacy are often justified on the grounds that they are necessary in order to ensure national security and prevent acts of terrorism. However, as is highlighted through the case law of the ECtHR and CJEU, despite the importance of this goal, the right to security does not justify unlimited infringements into the right to privacy. Rather, when necessary to do so, the Courts are happy to restrain this right.

Despite this fact, questions can be raised as to whether this approach is still appropriate in the modern digital world that we now all live. As more and more sources of data are produced, and subsequently collected, processed and analysed, the threat to the right to privacy only grows. As such, what the proportionality principle fails to consider is whether, rather than considering measures in isolation, we should be moving towards a more holistic method of assessing privacy interferences. As of yet, there is no recognised method through which this assessment could be conducted.

This article posits that the ecological concept of the ecosystem offers a manner through which this could be achieved. While the term ecosystem has found its way into common parlance, generally the benefits of utilising the full intricacy of the concept have failed to be recognised. This concept provides a method through which to map the various actors, recognise the interconnections and interactions between them, and acknowledge the prominent place that technology plays in this system. By adapting the concept for the legal field, the ecosystem offers a manner through which the law can balance competing interests, particularly when a variety of actors find themselves intricately linked and where the growing presence of technology plays an important role. In particular, it is posited that the adoption of the concept of a privacy ecosystem could enable a more proportionate balance between rights to be reached, by enabling those involved in assessing the proportionality of new measures, such as the courts, to take into account a wider range of 'interactions' than previously has been done. They could thus consider how the addition of a new measure to those already permitted might affect an individual's rights, as opposed to considering the measure by itself. After all, one of the key notions of the ecosystem is the recognition of the fact that the elements of the system cannot be analysed in isolation, but rather must be recognised for what they are – part of an interconnected

system. It is hoped that by doing so ultimately what shall be achieved is a better standard of human rights protection and greater fairness for the individual.

## Notes

1. For some, this might initially appear too Western-centric a statement. However, research supports the suggestion that most societies, both past, present, and even animal, value *some* form of privacy. Its form and importance varies across centuries, cultures and value structures, but its existence can be observed in almost all of them. For more detailed research into this area, Chapter One of Westin's *Privacy and Freedom* proves informative.
2. While not explicitly mentioned within the ECHR, the case law of the ECtHR has made it abundantly clear that the proportionality principle has a central importance to the protection of European human rights. See, e.g. Sunday Times v United Kingdom (1979) and Tsakyrakis (2009, 475).
3. Within the European Union, the principle of proportionality is explicitly established within Article 52 of the EU Charter.
4. See, e.g. Bundesverfassungsgericht, *Judgement of the First Senate of 2 March 2010*–1 BvR 256/08, para 218 https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2010/03/rs20100302_1bvr025608en.html (last accessed 13/01/2020).
5. While Tansley is commonly cited as establishing the ecosystem concept, credit for the actual term 'ecosystem' belongs to Arthur R. Clapham, who proposed the term after Tansley asked for suggestions for a term to describe the physical and biological components of an environment when considered together as part of a unit (Willis 1994; Ayres 2012).
6. The concept of 'systems' was commonly understood as describing the act of isolating a particular section of the universe for observation, and then watching to see how it changes after having been exposed to a variety of conditions. *See* Pickett and Grove (2009).
7. See, for example, Knight (2019) which highlights how Apple's failure to program gender into the algorithm which determined credit limits for their Apple Card resulted in discriminatory treatment. Other examples include Google's search algorithm spreading false information (Solon and Levin 2016) and algorithms creating racial discrimination in medical treatment (Johnson 2019). The effects that incorrect algorithms can have on an individual are wide ranging, and this is likely to only widen as they come to be relied upon more in the future. Particularly concerning is the fact that often it is not possible to identify why an algorithm worked in the manner in which it did.

## Disclosure statement

No potential conflict of interest was reported by the author(s).

## Funding

The author is an Early Stage Researcher within the ESSENTIAL ('Evolving Security SciencE through Networked Technologies, Information policy And Law') Project, the work of which is supported by the European Union's Horizon 2020 Research and Innovation Programme under the Marie Skłodowska-Curie Innovative Training Network (MSCA-ITN) Grant Agreement [Grant Number 722482]. The ideas herein reflect only the author's view.

## ORCID

*Lauren E. Elrick* http://orcid.org/0000-0003-4458-9745

## References


Agnellutti, C., ed. 2014. *Big Data: An Exploration of Opportunities, Values and Privacy Issues*. New York: Nova Science.

Aristotle. 2019. *Nicomachean Ethics*. 3rd ed. Indianapolis: Hackett.

Article 29 Data Protection Working Party, "Opinion 01/2014 on the Application of Necessity and Proportionality Concepts and Data Protection Within The Law Enforcement Sector". 2014. 536/14/EN WP 211, Accessed 10 January 2020. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf.

Ayres, P. 2012. *Shaping Ecology: The Life of Arthur Tansley*. Chichester: Wiley-Blackwell.

Baldwin, D. A. 1997. "The Concept of Security." *Review of International Studies* 23 (1): 5–26.

Barak, A. 2012. *Proportionality: Constitutional Rights and Their Limitations*. Cambridge: Cambridge University Press.

Bennett, C. J. 1991. "Computer, Personal Data, and Theories of Technology: Comparative Approaches to Privacy Protection in the 1990s." *Science, Technology and Human Values* 16 (1): 51–69.

Blackman, F. F., and A. G. Tansley. 1905. "Ecology in its Physiological and Phyto-Topographical Aspects – A Review." *New Phytologist* 4 (9): 232–253.

Broeders, D., E. Schrijvers, B. van der Sloot, R. van Brakel, J. de Hoog, and E. Hirsch Ballin. 2017. "Big Data and Security Policies: Towards a Framework for Regulating the Phases of Analytics and Use of Big Data." *Computer Law and Security Review* 33: 309–323.

Brown, I. 2009. "Terrorism and the Proportionality of Internet Surveillance." *European Journal of Criminology* 6 (2): 119–134.

Brown, A. E. 2019. *Intellectual Property, Climate Change and Technology: Managing National Legal Intersections, Relationships and Conflicts*. Cheltenham: Elgar.

Chandler, J. 2009. "Privacy Versus National Security: Clarifying the Trade-Off." In *Lessons From The Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, edited by Ian Kerr, Valerie Steeves, and Carole Lucock, 121–138. Oxford: Oxford University Press.

Clements, F. E. 1916. *Plant Succession: An Analysis of the Development of Vegetation*. Washington, DC: Carnegie Institute of Washington.

Coughlin, T. "175 Zettabytes By 2025" (Forbes, 27 November 2018). Accessed 1 May 2020. https://www.forbes.com/sites/tomcoughlin/2018/11/27/175-zettabytes-by-2025/.

Council of Europe. 2008. "Protecting the Right to Privacy in the Fight Against Terrorism." (4 December 2008) CommDH/IssuePaper 3.

Council of Europe. 2019. "Guide on Article 8 of the European Convention on Human Rights: Right to Respect for Private and Family Life, Home and Correspondence." (31 August 2019) Accessed 9 January 2020. https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf.

Couzigou, I. 2019. "Towards a State-Private Actor Partnership in Securing Cyberspace." University of Aberdeen, Research Centre for Constitution and Public International Law Working Paper Series 002/19.

DeCew, J. W. 2018. *In Pursuit of Privacy: Law, Ethics and the Rise of Technology*. Ithaca, NY: Cornell University Press.

Engle, E. 2012. "The History of the General Principle of Proportionality: An Overview." *The Dartmouth Law Journal* 10 (1): 1–11.

European Union Agency for Fundamental Rights. 2019. *Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement*. Accessed 1 May 2020. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf.

Feinberg, M. 2015. "International Counterterrorism – National Security and Human Rights: Conflict of Norms or Checks and Balances." *The International Journal of Human Rights* 19 (4): 388–407.

Fura, E., and M. Klamberg. 2012. "The Chilling Effect of Counter-Terrorism Measures: A Comparative Analysis of Electronic Surveillance Laws in Europe and the USA." In *Freedom of Expression – Essays in Honour of Nicolas Bratza – President of the European Council of Human Rights*, edited by Josep Casadevall, Egbert Myjer, and Michael O'Boyle, 463–481. Oisterwijk: Wolf Legal Publishers.

Gleason, H. A. 1917. "The Structure and Development of the Plant Association." *Bulletin of the Torrey Botanical Club* 44 (10): 463–481.

Golley, F. B. 1993. *A History of the Ecosystem Concept in Ecology: More Than The Sum Of The Parts*. New Haven, CT: Yale University Press.
Habermas, J. 1992. *The Structural Transformation of the Public Sphere: Inquiry Into a Category of Bourgeois Society*. Cambridge: Polity Press.
Harbo, T.-I. 2010. "The Function of the Proportionality Principle in EU Law." *European Law Journal* 16 (2): 158–185.
Himma, K. E. 2007. "Privacy Versus Security: Why Privacy Is Not An Absolute Value or Right." *San Diego Law Review* 44 (4): 857–920.
Hiranandani, V. 2011. "Privacy and Security in the Digital Age: Contemporary Challenges and Future Directions." *The International Journal of Human Rights* 15 (7): 1091–1106.
Hobbes, T. 2018. *Leviathan*. Minneapolis, MN: Lerner Publishing Group.
Hoffmann, P. 2004. "Human Rights and Terrorism." *Human Rights Quarterly* 26 (4): 932–955.
Johnson, C.Y. 24 October 2019. "Racial Bias in a Medical Algorithm Favours White Patients Over Sicker Black Patients." *Washington Post*, Accessed 1 May 2020. https://www.washingtonpost.com/health/2019/10/24/racial-bias-medical-algorithm-favors-white-patients-over-sicker-black-patients/.
Johnston, D. 2011. *A Brief History of Justice*. Chichester: Wiley-Blackwell.
Kaiser, C. 2018. "Privacy and Identity Issues in Financial Transactions: The Proportionality of the European Anti-Money Laundering Legislation." PhD thesis, University of Groningen, Groningen.
Klitou, D. 2014. *Privacy-Invading Technologies and Privacy by Design: Safeguarding Privacy, Liberty and Security in the 21st Century*. The Hague: T.M.C. Asser Press.
Knight, W. 19 November 2019. "The Apple Card Didn't 'See' Gender – And That's The Problem." (Wired). Accessed 1 May 2020. https://www.wired.com/story/the-apple-card-didnt-see-genderand-thats-the-problem/.
Kolodziej, E. A. 2005. *Security and International Relations*. Cambridge: Cambridge University Press.
Lazarus, L. 2015. "The Right to Security." In *Philosophical Foundations of Human Rights*, edited by Rowan Cruft, S. Matthew Liao, and Massimo Renzo, 423–441. Oxford: Oxford University Press.
Levy, H. 1932. *The Universe of Science*. London: C.A. Watts.
Locke, J. 1948. "An Essay Concerning the True Original, Extent and End of Civil Government." In *The Second Treatise of Civil Government and A Letter Concerning Toleration*, edited by John W. Gough. Oxford: Basil Blackwell.
Mars, M. M., and J. L. Bronstein. 2018. "The Promise of the Organizational Ecosystem Metaphor: An Argument for Biological Rigor." *Journal of Management Inquiry* 27 (4): 382–391.
McIntosh, R. P. 1985. *The Background of Ecology: Concept and Theory*. Cambridge: Cambridge University Press.
McIntosh, R. P. 1998. "The Myth of Community as Organism." *Perspectives in Biology and Medicine* 41 (3): 426–438.
Milaj, J. 2016. "Privacy, Surveillance and The Proportionality Principle: The Need For A Method of Assessing Privacy Implications of Technologies Used For Surveillance." *International Review of Law, Computers and Technology* 30 (3): 115–130.
Mitsilegas, V. 2015. "The Transformation of Privacy in an Era of Pre-Emptive Surveillance." *Tilburg Law Review* 20 (1): 35–57.
Moeckli, D. 2008. *Human Rights and Non-Discrimination in the 'War on Terror'*. Oxford: Oxford University Press.
Norris, T. B., and T. Suomela. 2017. "Information in the Ecosystem: Against the "Information Ecosystem"." *First Monday* 22 (9). doi:10.5210/fm.v22i9.6847.
Odum, E. P. 1971. *Fundamentals of Ecology*. 3rd ed. Philadelphia, PA: W.B. Saunders.
Pickett, S. T. A., and M. L. Cadenasso. 2002. "The Ecosystem as a Multidimensional Concept: Meaning, Model and Metaphor." *Ecosystems* 5: 1–10.
Pickett, S. T., and J. M. Grove. 2009. "Urban Ecosystems: What Would Tansley Do?" *Urban Ecosystems* 12: 1–8.
Platjouw, F. M. 2016. *Environmental Law and the Ecosystem Approach: Maintaining Ecological Integrity Through Consistency in Law*. New York: Routledge.

Russell, J. A., W. H. Peters, N. N. Craig, and B. C. Coull. 2006. "Systems and Ecosystems." In *Sustainability Science and Engineering: Defining Principles*, edited by Martin A. Abraham, 113–126. Amsterdam: Elsevier.
Scassa, T. 2017. "Law Enforcement in the Age of Big Data and Surveillance Intermediaries: Transparency Challenges." *SCRIPTed* 14 (2): 239–284.
Schneier, B. 2015. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York: W.W. Norton.
Serwin, A. B. 2009. "Privacy 3.0 – The Principle of Proportionality." *University of Michigan Journal of Law Reform* 42 (4): 869–930.
Shue, H. 1996. *Basic Rights: Subsistence, Affluence and U.S Foreign Policy*. 2nd ed. Princeton, NJ: Princeton University Press.
Solon, O. & Levin, S. 16 December 2016. "How Google's Search Algorithm Spreads False Information with a Rightwing Bias." *The Guardian*. Accessed 1 May 2020. https://www.theguardian.com/technology/2016/dec/16/google-autocomplete-rightwing-bias-algorithm-political-propaganda.
Tansley, A. G. 1935. "The Use and Abuse of Vegetational Concepts and Terms." *Ecology* 16 (3): 284–307.
Tsakyrakis, S. 2009. "Proportionality: An Assault on Human Rights?" *International Journal of Constitutional Law* 7 (3): 468–493.
United Nations Human Rights Council. 2009. "Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, Martin Scheinin." (28 December 2009) UN Doc. A/HRC/13/37.
United Nations Human Rights Council. 2016. "Report of the Special Rapporteur on the Right to Privacy, Joseph A. Cannataci." (24 November 2016) UN Doc. A/HRC/31/64.
Valkenburg, G. 2015. "Privacy Versus Security: Problems and Possibilities for the Trade-Off Model." In *Reforming European Data Protection Law*, edited by Serge Gutwirth, Ronald Leenes, and Paul de Hert, 253–269. Dordrecht: Springer.
Van der Valk, A. G. 2014. "From Formation to Ecosystem: Tansley's Response to Clements' Climax." *Journal of the History of Biology* 47: 293–321.
Van Gerven, W. 1999. "The Effect of Proportionality on the Actions of Member States of the European Community: National Viewpoints From Continental Europe." In *The Principle of Proportionality in the Laws of Europe*, edited by Evelyn Ellis, 37–64. London: Hart Publishing.
Wæver, O. 2011. "Securitization." In *Security Studies: A Reader*, edited by Christopher W. Hughes and Lai Yew Meng, 93–98. London: Routledge.
Westin, A. 1967. *Privacy and Freedom*. New York: Ig Publishing.
Willis, A. J. 1994. "Arthur Roy Clapham, 24 May 1904–18 December 1990." *Biographical Memoirs of Fellows of the Royal Society* 39: 71–90.
Willis, A. J. 1997. "The Ecosystem: An Evolving Concept Viewed Historically." *Functional Ecology* 11 (2): 268–271.
Wolfers, A. 1952. "National Security" as an Ambiguous Symbol." *Political Science Quarterly* 67 (4): 481–502.
Woolley, O. 2014. *Ecological Governance: Reappraising Law's Role in Protecting Ecosystem Functionality*. Cambridge: Cambridge University Press.
Woolley, O. 2020. "What Would Ecological Climate Change Law Look Like? Developing A Method for Analysing the International Climate Change Regime From An Ecological Perspective." *Review of European, Comparative and International Environmental Law* 29 (1): 76–85.

### *Legislation*

UN General Assembly, Universal Declaration of Human Rights (10 December 1948) Res. 217 A(III).
United Nations, International Covenant on Civil and Political Rights (16 December 1966) UNTS vol.999, pg.171.
Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14 (4 November 1950) ETS 5.
European Union, Charter of Fundamental Rights of the European Union (26 October 2012), 2012/C326/02.

***Case Law (ECtHR)***

Handyside v United Kingdom [1976] ECHR 5
The Sunday Times v United Kingdom (No.1) [1979] ECHR 1
Dudgeon v United Kingdom [1981] ECHR 5
Silver and Others v United Kingdom [1983] ECHR 5
X and Y v Netherlands [1985] ECHR 4
Olsson v Sweden (No.1) (1988) 11 EHRR 259
Gaskin v United Kingdom [1989] ECHR 13
Soering v United Kingdom [1989] ECHR 14
Niemietz v Germany [1992] ECHR 80
Keegan v Ireland [1994] 18 EHRR 342
Z v Finland [1997] ECHR 10
X, Y and Z v United Kingdom [1997] ECHR 20
Christine Goodwin v United Kingdom [2002] ECHR 588
Peck v United Kingdom [2003] ECHR 44
Odièvre v France [2003] ECHR 86.
Segerstedt-Wiberg and Others v Sweden [2006] ECHR 597
S and Marper v United Kingdom [2008] ECHR 178
Gardel v France [2009] ECHR 16428/05
Hämäläinen v Finland [2014] ECHR 877
Mozer v Republic of Moldova and Russia [2016] ECHR 213
Bărbulescu v Romania [2017] ECHR 742
Libert v France (2018) ECHR 185

***Case Law (CJEU)***

Joined Cases C-293/12 Digital Rights Ireland and C-594/12 Seitlinger and Others [2014] ECLI:EU:C:2014:238
Joined Cases C-203/15 Tele2 Sverige and C-698/15 Watson and Others [2016] ECLI:EU:C:2016:970