Philos. Technol. (2013) 26:381–395
DOI 10.1007/s13347-013-0119-6

SPECIAL ISSUE

Online Security and the Protection of Civil Rights: A Legal Overview

Ugo Pagallo

Received: 24 January 2013 / Accepted: 28 June 2013 / Published online: 17 July 2013

Abstract The paper examines the connection between online security and the protection of civil rights from a legal viewpoint, that is, considering the different types of rights and interests that are at stake in national and international law and whether, and to what extent, they concern matters of balancing. Over the past years, the purpose of several laws, and legislative drafts such as ACTA, has been to impose "zero-sum games". In light of current statutes, such as HADOPI in France, or Digital Economy Act in UK, the paper intends to illustrate how more satisfactory solutions are feasible in the field of online security, such as the new "Police and Criminal Justice Data Protection Directive" that the European Commission presented in January 2012. At least in Western legal systems, it should be clear that either civil rights prevail over security (no balancing), or such balance has to satisfactorily protect individual rights (proportionality).

Keywords Civil rights · Data protection · Filtering systems · Legal balancing · Online security · Privacy by design · Self-enforcing technologies

1 Introduction

This paper dwells on the different ways in which lawyers describe, examine, and argue about the connection between online security and civil rights. The debate includes advocates of the "security first" and "liberty first" theses, supporters of self-enforcing technologies, digital rights management (DRM) techniques, and systems of filtering on the internet, much as promoters of new rights that involve, say, the individual access to the net. From a legal point of view, the complexity of the subject matter revolves around two crucial issues, namely, the different types of rights and interests that are at stake and whether, and to what extent, they regard matters of legal balancing. By drawing the attention to the hierarchical structure of the law and how we should interpret the nature and logic of the principles of the system, think of multiple types of rights, such as

U. Pagallo (✉)
Law School, University of Torino, via s. Ottavio 54, 10124 Turin, Italy
e-mail: ugo.pagallo@unito.it

(a) Natural rights, in accordance with the philosophical tradition of contractualism and liberalism, e.g. John Locke's *Two Treatises of Government*
(b) Human rights in the field of international law, e.g. the European Convention on Human Rights ("ECHR") from 1950
(c) Constitutional rights of national legal systems, such as the civil rights of the US tradition or, conversely, the fundamental rights of the EU law and its Member States, and
(d) Rights established by statutory laws

This differentiation is fruitful so as to start appreciating the different levels of protection concerning the rights of the individuals. On the one hand, ordinary or statutory laws (*sub d*) are subordinated to the provisions and principles of constitutional law (*sub c*) and, at times, of international law (*sub b*). On the other hand, national constitutional laws often provide for a stronger, or more efficient, level of protection than terms and conditions of international law. Yet, such provisions and principles of constitutional law vary according to the traditions of multiple legal systems, so that we should further differentiate between, say, the US tradition of civil rights, e.g. freedom of speech under the First Amendment protection, and the EU legal framework, e.g. the individual right to data protection conceived of as a fundamental right (Pagallo 2008). In this context, these differences are taken into account if, and only if, they help us understand whether issues of online security and the protection of such rights as natural, human, constitutional, or statutory rights involve matters of legal balancing. Thus, for the sake of conciseness, these rights are most of the time considered here as equivalent and succinctly dubbed as "civil rights". Although the formula may sound as too American, the notion stands for the rights that the individuals should enjoy in the "civil society", according to the jargon of modern contractualism. On this basis, we then have to determine whether, and to what extent, the different types of rights and interests that are at stake in the fields of national and international law, constitutional law, transnational law, etc., have to be balanced in the name of security.

Focus is again on the hierarchical structure of the law and, moreover, on how we should interpret the nature and logic of the principles of the system in the case of online security. Although for opposite reasons, advocates of both the "security first" and "liberty first" theses claim that the aim to enforce online security or vice versa, to protect civil rights trump each other and, consequently, do not involve trade-offs: among advocates of the "security first" thesis suffice it to mention Thomas Hobbes (ed. 1999) and, more recently, Amitai Etzioni (2007); among the most famous theorists of the "liberty first" thesis, John Locke (ed. 1988). Hence, from this point of view on the political foundations of legal interaction, attention is drawn to the connection between collective (or national) security *and* the protection of civil rights, whereas such "and" crucially functions either as a disjunction (e.g. Hobbes) or a conjunction (e.g. Locke), between the terms of the relation. They could be grasped as the ends of a spectrum.

Still, we should further distinguish between "absolute" and "relative" rights. Contemplate the aforementioned 1950 European Convention on Human Rights ("ECHR") and the difference between absolute rights (e.g. protection from retrospective criminal penalties) and relative rights (e.g. privacy). In the case of absolute

human (or civil) rights, the distinction between principles and values suggested by Jürgen Habermas in *Facts and Norms* (1996) is fruitful, because principles can be deemed as normative statements having a deontological, rather than teleological, meaning: in other words, some principles (such as the principle of legal responsibility) follow the logic of yes or no, or that which is for the good of all, contrary to the logic of that which is good for us, or good more or less, that characterizes values (Habermas 1996). This logic of yes or no—as opposed to every notion of legal balancing—appears time and again in this paper. In light of today's debate on the current responsibilities of internet service providers (ISPs), as examined below in Sections 4 and 6, think of the Latin expression, *nullum crimen nulla poena sine lege*, that is, no punishment is legitimate without law: an individual's criminal responsibility is subordinated to the existence of a specific norm or statute in accordance with the principle of legality and its Anglo-Saxon counterpart, the rule of law.

This logic of yes or no, however, hardly fits the case of relative human rights: here, lawyers do often balance rights and interests, e.g. individual privacy and national security, according to the logic of more or less that characterizes, say, the case law of the European Court of Human Rights ("EHCR") in the name of further principles, as the principle of proportionality, predictability, and necessity. In this latter case, lawyers are closer, say, to the thesis of Ronald Dworkin (1985), than Habermas (1996), because the aim would be to achieve certain goals to their maximum degree through the principles of the system. This does not mean, of course, that the protection of relative civil rights always entails matters of balancing, and what is more, a number of scholars and private firms claim that determining social behaviour through the use of such techniques as DRMs, TPMs, filtering systems, and other types of self-enforcing technologies is lawful. As a result, the polarization between advocates of the "security first" and "liberty first" theses in the political field, i.e. the Hobbesian and Lockeian versions of the social covenant, re-emerges in both the field of private, rather than public, law and matters of private and collective security that have to be determined through the design of the environment of social interaction, e.g. interaction on the internet. These issues have been discussed before the EU Court of Justice in *Scarlet Extended* (C-70/10) and *Netlog* (C-360/10), and they represent the core of what is legally at stake with some recent statutes, such as the UK Digital Economy Act ("DEA") from 2010. In order to enforce the security of online services, is it legitimate to install a filtering system such as the information system discussed in the Netlog case? Is it lawful the use of DRMs, once we consider, say, antitrust issues (Jobs 2007)? Vice versa, is it feasible to enforce online security and, nonetheless, strengthen the protection of civil rights? Moreover, *how* would it be possible?

In order to offer a hopefully comprehensive picture of today's debate, let me conceive the spectrum of opinions and legal acts as falling within the ends of such spectrum: these ends define crucial cases that need no legal balance. By taking into account some legal differences between norms and principles that govern the interaction between public *and* private actors, *between* private individuals, and *within* public/private architectures, the different ways in which lawyers describe, examine, and argue about the connection between online security and civil rights can be summed up in light of three different spectra. From a legal viewpoint, they are defined by the ends of

(a) National security and the protection of civil rights, as examined below in Section 2
(b) Individual security and the protection of further private rights, which are under scrutiny in Section 3
(c) Private and public security via design vis-à-vis the protection of civil rights on the internet, as illustrated in Section 4

On this basis, in Section 5, the purpose is to stress that which these different levels of analysis may have in common, namely, conceiving issues of online security and the protection of civil rights either as a "zero-sum game" or, conversely, through "win–win" approaches. The first no-balancing option is illustrated by the use of self-enforcing technologies, DRM and TPM techniques, or digital firewalls that admit no interface between the law's terms and its application (Zittrain 2007). At the other end of the spectrum, the alternative no-balancing option is given by Ann Cavoukian's version of the principle of privacy by design. Here, personal data should automatically be protected in every IT system as its default position, by embedding data protection safeguards into the design of such systems: the full functionality of the principle would allow a positive-sum game, making trade-offs unnecessary, e.g. privacy vs. security (Cavoukian 2010). However, since a number of cases arguably fall in between the ends of this spectrum, i.e. between zero-sum and positive-sum games, Section 5 dwells on how the different types of rights and interests mentioned above are often balanced in the fields of international law (e.g. the case law of the ECHR on privacy *and* security), constitutional law (e.g. the aforementioned differences between the US tradition of civil rights and the EU legal framework of fundamental rights), and even transnational law (e.g. internet governance and the decisions of ICANN as a legal source of the system).

Still, we will see a new set of cases that fall within the loopholes of current legal systems, e.g. an individual right to online access and the neutrality of the services on the internet. Section 6 aims to explain why some of today's trends are quite alarming: on one hand, matters of online security are suggesting private companies and some hundred million people alike to opt for more reliable, yet sterile, appliances, e.g. tablets, e-books, and video game consoles. On the other hand, as technology transfigures the essence of traditional legal issues, such as privacy, copyright, or the neutrality of ISP services, lawmakers have often overreacted to this new scenario. Rather than a fair balance between rights and interests, let aside win–win approaches, the aim of several laws, and legislative drafts such as ACTA, has been to impose zero-sum games. Against this trend, the purpose of this paper is not only to offer a map of the different ways in which lawyers describe, examine, and argue about issues of online security and the protection of civil rights: in light of such current statutes, as HADOPI in France, or DEA in UK, the paper intends to illustrate how more satisfactory solutions are feasible in the field of online security, by exploring and exploiting the full spectrum of legal options at hand.

2 National Security and Civil Rights

The first step of the analysis has to dwell on that "and" which functions either as a conjunction or as a disjunction, between online security *and* civil rights. In the first case, security should be numbered among the rights of the individual, in accordance

with the "social covenant" of John Locke, or when security is grounded on voluntary agreements between the parties to a contract, e.g. your online bank account and the obligation of the bank to deliver safe services. Vice versa, a twofold differentiation is necessary in the second case, namely, the distinction between national security and civil rights on one side and, on the other, between individual security and further private rights. In light of this twofold differentiation, let us start with the notion of national or public (as opposed to private) security and the ways in which the aim to guarantee national or collective security is connected to the protection of individual rights. This is, of course, the paramount topic of modern constitutionalism, much as of liberalism, or democratic theory. Here, the topic can be summarized with a first polarization. At one end of the spectrum, it suffices to mention some aspects of the political philosophy of Thomas Hobbes, at the other, the aforementioned social covenant of John Locke.

A classical text, such as Hobbes's *Leviathan*, illustrates the reasons why we should conceive the "and" between national security and civil rights disjunctively, and moreover, the aim to guarantee such security has to have legal priority. In the wording of chapter XVII of *Leviathan*, "the final cause, end, or design of men (who naturally love liberty, and dominion over others) in the introduction of that restraint upon themselves, in which we see them live in Commonwealths, is the foresight of their own preservation." In order to overcome the condition of insecurity and war, summed up as the state of nature, a multitude of men agree via the social covenant that the sovereign has the right to determine what the law is in the civil society. In the phrasing of chapter XVIII, "a Commonwealth is said to be instituted when a multitude of men do agree, and covenant, every one with every one, that to whatsoever man, or assembly of men, shall be given by the major part the right to present the person of them all, that is to say, to be their representative."

Admittedly, some tenets of this Hobbesian political representation are controversial: for instance, scholars still discuss whether or not Hobbes should be conceived as a "liberal" thinker (Strauss 1936). According to some interpretations of the *Leviathan*, citizens have the faculty to decide whether they should obey certain of the sovereign's commands in the "foresight of their own preservation". After all, this was the interpretation of some contemporaries of Hobbes, such as Filmer, Clarendon, and Bishop Bramhall in *The Catching of the Leviathan* (1658), where the latter dubs Hobbes's book as a "Rebel's catechism". Consider what the famous and problematic sentence of chapter XXI of *Leviathan* states: "When therefore our refusal to obey frustrates the end for which the sovereignty was ordained, then there is no liberty to refuse; otherwise, there is." However, regardless of the intricacies of Hobbes's work, it seems fair to affirm that the limits to the sovereign's will are a matter of power (*de facto*), rather than law (*de iure*); they concern the liberty, rather than the civil rights, of the subjects. This approach has, more recently, been endorsed by a number of Western scholars, such as Amitai Etzioni in *Security First* (2007): providing basic security must be the first priority in policy considerations, at least in international affairs, because security drives democracy, and not the other way around.

At the other end of the spectrum, Locke's *Two Treatises* offer an alternative stance on law and politics, since individuals give up the natural right to self-defence in order to enforce their "property" in the civil society, which includes the natural rights to life and liberty. These rights represent the fundamental (legal and constitutional) limits to all of the ruler's decisions, contrary to Hobbes's ideas on sovereignty, security and

individual rights: "For if it be asked what security, what fence is there in such a state against the violence and oppression of this absolute ruler, the very question can scarce be borne" (*Second Treatise*, Ch. VII, sec. 93). Although security is the precondition for the enforcement of such absolute rights, as the Lockean right to life in the civil society, there is no way of balancing this right against the need of guaranteeing collective security, let alone the sacrifice of the right to life in the name of national safety. Here, *pace* Hobbes, the limits of political power are legally defined by the law of nature (*de iure*), rather than factual arguments (*de facto*); they concern what today's scholars define as human rights in the international law field, civil rights in the US constitutional law field, fundamental rights in the EU law field, etc. In a nutshell, according to Locke, "freedom of Men under Government is, to have a standing Rule to live by, common to every one of that Society, and made by the Legislative Power erected in it; a Liberty to follow my own Will in all things, where the Rule prescribes not; and not to be subject to the inconstant, uncertain, unknown, Arbitrary Will of another Man: as Freedom of Nature is, to be under no other restraint but the Law of Nature" (*Second Treatise*, Ch. IV, sec. 22).

To be fair, some aspects of Locke's legal and political philosophy are still controversial, such as the connection between law of nature and natural rights, the possible conflict between the legislative power and the will of the subjects, and so on. However, complementary to Hobbes's ideas, it is apparent that matters of security and individual rights do not necessarily raise problems of balancing in Locke's analysis. By following a Hobbesian approach, no trade-off is needed between security and natural (or civil, or human, or constitutional, or fundamental) rights, because "priority first", in Etzioni's phrasing. Vice versa, by endorsing a liberal standpoint, we end up with cases in which security and individual rights cannot be balanced for opposite reasons. Reflect on Article 3 of the European Convention on Human Rights and the prohibition of torture: "No one shall be subjected to torture or to inhuman or degrading treatment or punishment." Likewise, consider protection from retrospective criminal penalties, as mentioned above in the introduction. This logic of yes or no applies to the field of online security as well: although matters of balance between online security and civil rights call for the protection of relative (rather than absolute) individual rights, we have seen in the introduction that the protection of relative civil rights does not necessarily entail trade-offs. This differentiation can be further illustrated with the jurisprudence of the EU Court of Justice: even though the latter often resorts to the idea of legal balancing, as examined below in Section 5, some relative rights shall not be balanced, e.g. the right to the protection of personal data in *Scarlet Extended* (C-70/10). As such, this type of rights that individuals enjoy in the civil society represent, so to speak, the liberal end of the first spectrum. Against the "Security first" thesis, let us dub this position as the "Liberty first" approach.

3 Private Security and Other Civil Rights

After the "Security first" and "Liberty first" theses on the political foundations of legal interaction, e.g. the Hobbesian and Lockeian versions of the social covenant, the second polarization of the debate concerns the legal interaction of private actors, that is, how the protection of private (rather than public, or national) security is related to the protection of further individual rights. The opinions of the debate can be summarized with a new

spectrum, at the ends of which no balance has to be struck. At one end of the spectrum, online security and civil rights pit against each other in a zero-sum game: consider the aim of private companies to protect their rights through the use of self-enforcing technologies, e.g. DRM devices. By enabling right holders to monitor and regulate the use of their copyright-protected works, companies would prevent unsolvable problems concerning both the enforceability of national norms and the conflicts of law at the international level. Whilst, in his *Thoughts on Music* (2007), Steve Jobs conceded that DRM-compliant systems raise severe challenges of interoperability and, hence, antitrust issues, there are two further reasons why the use of DRM techniques appears particularly controversial. First, as a response to the inefficacy of state action on the internet, DRM technology risks to severely curtail individual freedom and collective autonomy, since people's behaviour would unilaterally be determined on the basis of technology, rather than by choices of the relevant political institutions. Second, the use of self-enforcing technologies ultimately impinges on people's right to have a say in the decisions affecting them, for a kind of infallible self-enforcement technology collapses "the public understanding of law with its application eliminating a useful interface between the law's terms and its application" (Zittrain 2007). In a nutshell, DRMs are highly controversial from a legal viewpoint, because the aim to prevent every sort of balancing between the interest of right holders to strictly regulate the use of their own copyright-protected works and the protection of such civil rights as freedom of speech, fair use, and so forth is clear.

At the other end of the spectrum, security is conceived as an individual right that is grounded, in most of the cases, on voluntary agreements between the parties to a contract. As mentioned above in the introduction, think of online bank accounts and the obligation of banks to deliver safe services. Here, the individual right to safety goes hand in hand with her security, so much so that some consider such notions as interchangeable as, for example, the US Department of Homeland Security's website is keen to argue. Vice versa, others insist on the difference between the notions of security and safety, in that "a safety critical system is one whose failure could do us immediate, direct harm", whereas "a security critical system is one whose failure could enable, or increase the ability of, others to harm us" (Burns et al. 1992). This differentiation between the individual right to safety and the right to individual security is fruitful, because there are several cases where security and safety have to be balanced. A typical instance is given by the processing of personal data in hospitals via information systems, whereas patient names should be kept separated from data on medical treatments or health status. Should we privilege the efficacy and reliability of that information system in keeping patient names separated from data on medical treatments or health status? How about users, including doctors, who may find such mechanism too onerous?

However, by distinguishing between safety and security systems, it does not follow that such relative rights, as an individual right to safety and her right to security, should always be balanced against each other. On the contrary, many cases suggest that the aim to guarantee individual security, and safety, goes hand in hand with the protection of further civil rights of the individual. This usually occurs when legal interaction between private actors entails collaboration or their interests converge, e.g. the aims to prevent both the failures of a safety critical system and of a security critical system overlap. From this further outlook, no necessary trade-offs between security and civil rights are at stake,

much as it occurs with the Lockean perspective on collective security as the precondition to safely enjoy the natural right to life, freedom, and property in the civil society (as seen in the previous section). In both cases, there is no room for balancing: in addition to rights that are absolute in the public law field, security and safety are typical rights of the individual that, although "relative", do not necessarily entail a zero-sum game between private actors. Rather, the aim of such actors to guarantee online security may fit like hand to glove with the protection of further civil rights. Besides the example of online bank services mentioned above, this is what we expect from a number of further online services on the internet, namely that which is summed up as a win–win scenario below in Section 5.

4 Security by Design and the Protection of Civil Rights on the Internet

After norms and principles that govern social interaction *within* the public field, or *between* private actors, the third level of the analysis has to do with the environment of both public and private interaction, much as the architecture, or design, of such environment. Again, the opinions in the debate can be conceived as falling within the ends of a spectrum that concerns public authorities requiring private companies to ensure online security, e.g. ISPs as sheriffs of the net and, vice versa, private companies lobbying public authorities to enforce their own rights and interests via the use of, say, filtering systems on the internet. At one end of the spectrum, security trumps civil rights through the use of such filtering systems, because no balancing would be possible between the aim to ensure online security via this technique and the protection of some basic rights, such as data protection, freedom of speech and of information, freedom to conduct a business, and so forth. At the other end of the spectrum, there are constitutional limits to the use of such filtering systems in order to protect some of the basic rights mentioned above. Two decisions of the EU Court of Justice, namely *Scarlet Extended* (C-70/10) and Netlog (C-360/10), are instructive to further illustrate the ends of this spectrum. In both cases, the plaintiff was a management company, SABAM, which represents authors, composers, and publishers of musical works in Belgium. As such, SABAM is responsible for authorizing the use by third parties of copyright-protected works of these authors, composers, and publishers. By claiming that an internet service provider, i.e. Scarlet, and then a social network, Netlog, made such works available to the public without SABAM's consent and without paying it any fee, the plaintiff requested the Court of First Instance in Brussels an injunction against the defendants in order to take appropriate measures to stop the infringement of the plaintiff's intellectual property (IP) rights and, moreover, to prevent any further infringement.

In the case of Netlog, the national court would have had to issue an injunction against the social network requiring the latter to install a system that, in the wording of the EU Court of Justice, should filter:

(a) "Information which is stored on its servers by its service users;
(b) Which applies indiscriminately to all of those users;
(c) As a preventive measure;
(d) Exclusively at its expense; and
(e) For an unlimited period;

Which is capable of identifying electronic files containing musical, cinematographic or audio-visual work in respect of which the applicant for the injunction claims to hold intellectual property rights" (C-360/10).

On 16 February 2012, the Court ruled that such filtering system is precluded by the EU directives on e-commerce (2000/31/EC), copyright (2001/29/EC), and IP (2004/48/EC), much as data protection (1995/46/EC) and the freedom to receive or impart information, according to Articles 8 and 11 of the EU Charter of Fundamental Rights. "Moreover, that injunction [to install the filtering system] could potentially undermine freedom of information, since that system might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications" (C-260/10). It follows that, in order to protect these basic rights, the type of security by design, at stake in Netlog, is illegitimate. By quoting its case law (C-275/06, that is, *Promusicae*), the Court affirms that none of the rights to intellectual property are either "inviolable" or "absolute", but, rather, they should be "balanced against" the protection of other fundamental rights. Yet, it is noteworthy that no balancing was needed in Netlog. In the phrasing of the Court, the EU law "must be interpreted as precluding a national court from issuing an injunction against a hosting service provider which requires it to install a system for filtering", as the system described above.

At the end of the day, however, it is still unclear what type of security by design would ultimately be legitimate in EU law. Some controversial provisions of the UK DEA from 2010 illustrate the point, in that an "initial obligations code" should impose on ISPs the duty to notify subscribers of copyright infringement reports received from copyright owners and to provide copyright infringement lists to copyright owners, in addition to some "technical obligations", some of which included a "technical obligations code". Certain ISPs, such as British Telecom, claim that such provisions are illegitimate pursuant to EU directives on data protection, copyright, freedom to conduct a business, and so forth. To date, nevertheless, two British courts have endorsed the opinion of some powerful copyright holders. In the wording of the Court of Appeal in London, on 6 March 2012, "a certain amount of energy was expended before us on the recent judgement of the Court of Justice in *Scarlet*… which concerned the compatibility with the Privacy and Electronic Communications Directive and other directives of a court injunction against an ISP requiring it to install a system for filtering electronic communications in order to identify and block the transfer of files infringing copyright. Both the Advocate General and the Court referred to *Promusicae*, in terms that do not in my view cast any great light on that ruling; but I see nothing in the case to support the limited scope that the applicants seek to give to the ruling in *Promusicae*" (CI/2011/1437, n. 82).

Whether or not we agree with the Court, both ends of the third spectrum should be clear. At one end, there is the binary logic of filtering systems that admit no balance, since they "identify and block the transfer of files infringing copyright", in the words of the Court of Appeals in London. At the other end of the spectrum, the ruling of *Scarlet* illustrates cases in which the protection of basic civil rights require this logic of yes or no, so that some filtering systems should be deemed as illegitimate. Such opposite ways to come to the same conclusion, i.e. no balancing, are deepened in the next section.

5 Zero-Sum Games and Win–Win Approaches

This section draws the attention to that which the previous levels of the analysis may have in common, i.e. what the mediaeval scholars used to call *genus proximum*, as dialectically opposed to the *differentia specifica* between the ends of the spectra examined in the previous sections. At one end of this final spectrum, no balance has to be struck between security and civil rights, because some Hobbesian approaches to national security, as seen above in Section 2, much as the use of self-enforcing technologies and systems of filtering on the internet, as described in Sections 3 and 4, involve a zero-sum game. Similarly, at the other end of the spectrum, no balancing is needed because the protection of some basic rights, either absolute (Section 2) or relative (Section 4), in addition to forms of collaborative interaction (Section 3), preclude such a balance or entail a win–win scenario. Consider, for instance, some versions of the principle of "privacy by design" (Pagallo 2012a, b): personal data should be automatically protected in every IT system as its default position, so that a cradle-to-grave, start-to-finish, or end-to-end lifecycle protection ensures that privacy safeguards are at work even before a single bit of information has been collected. By embedding privacy safeguards into the design of ICTs, the full functionality of the principle would allow a positive-sum or win–win game, making trade-offs unnecessary between security and civil rights (Cavoukian 2010).

Admittedly, the aim of guaranteeing security can fit like hand to glove with the protection of civil rights through the approach of the principle of privacy by design, e.g. making personal data anonymous in public transportation systems through video surveillance that must be designed in such a way that faces of individuals cannot be recognizable. Yet, this win–win approach has its problems: on the one hand, the limits of the automatic protection of people's privacy bring us back to the reasons why the use of self-enforcing technologies can be so tricky. As mentioned above in Section 3, there is the risk of curtailing freedom and individual autonomy severely, because people's behaviour would be determined on the basis of design rather than by individual choices: "the controls over access to content will not be controls that are ratified by courts; the controls over access to content will be controls that are coded by programmers" (Lessig 2004). On the other hand, current work on legal ontologies, value-sensitive design, P3P or PeCAM platforms show the limits of today's state of the-art in technology: these limits depend on the difficulty of modelling highly context-dependent normative concepts that do not entail zero-sum games but concern personal choices about levels of access and control over information, which often hinge on the circumstances of the context. In the phrasing of Karen Yeung (2007), "a rich body of scholarship concerning the theory and practice of 'traditional' rule-based regulation bears witness to the impossibility of designing regulatory standards in the form of legal rules that will hit their target with perfect accuracy."

As a result, striking a balance between security and civil rights seems necessary in a number of legal cases that fall in between the ends of the spectrum, that is, between zero-sum games and win–win scenarios. In light of the different types of interaction stressed above, i.e. public *and* private (Section 2), *between* private individuals (Section 3), and *within* public/private architectures (Section 4), consider three examples of balancing:

(a) Between national security and such a human right as the right to privacy in the jurisprudence of ECHR. Here, the balance revolves around what is "necessary" pursuant to Article 8 of the Convention in *Gillow vs*. *UK* from 24 November 1986, § 55; or, in *Leander vs*. *Sweden* from 26 March 1987, § 59. Likewise, think of the principle of "predictability" in *Olsson vs*. *Sweden* from 24 March 1988 and the indispensable balance between what is necessary in a democratic society in the interests of national security and people's right to respect for their private life (*Klass* et al. *vs*. *Germany*, 6 September 1978, § 59)

(b) Between the individual right to security and how this right to, say, self-defence and safety has to be balanced with further constitutional rights. Some striking differences between the US approach to this (gun) right and most of the European legal systems should be stressed

(c) Between fundamental rights and the new environment of public/private interaction in the jurisprudence of the EU Court of Justice. As mentioned above in Section 4, in light of the *Promusicae* case, there is not only the need of striking a "fair balance" between such fundamental rights as copyright and privacy. Besides, the use of filtering systems for both public and private purposes should not curtail the protection of some further basic rights, such as freedom of speech and of information, freedom to conduct a business, etc.

This case law sheds light on crucial differences between national constitutional laws and international law that should be taken into account when focusing on issues of online security and the protection of civil rights. However, as technological progress reshapes key assumptions in legal arguments, the information revolution induces a new set of cases that fall within the loopholes of current legal systems. Consider the notion of "neutral services" on the internet as well as whether individuals have the right to access to the net. These issues are examined separately in the next section: the aim is to stress that lawmakers have often overreacted to the challenges of the information revolution, by favouring certain technical and political choices over others. Rather than a fair balance between rights and interests, let aside win–win scenarios, the purpose of an increasing number of laws, or legislative drafts such as ACTA, has been to impose zero-sum games.

6 New Scenarios

It is still an open question whether methods of automated filtering of information are compatible with the "neutrality" of services, on which the responsibility of ISPs depends in such sectors as keyword advertising, trade marks, search engines, social networks, and the like. So far, the clause of legal immunity for ISPs has been granted by both the US and EU lawmakers, to strengthen the flow of information on the internet pursuant to Section 230 of the US *Communication Decency Act* from 1996, Section 512 (c) of the US *Digital Millennium Copyright Act* (DMCA) from 1998, and the responsibility regime set up by the EU Directive 2000/31/EC on e-commerce. According to article 15 of this latter directive, there is no general obligation for ISPs to monitor the information which they transmit or store, "nor a general obligation actively to seek facts or circumstances indicating illegal activity".

Yet, as declared by the European Court of Justice in the *Google v. Louis Vuitton case* on 23 March 2010, liability of online referencing service providers ultimately depends on "the actual terms on which the service is supplied". In other words, according to the judges in Luxembourg, it is necessary to determine "whether the role played by that service provider is neutral, in the sense that its conduct is merely technical, automatic and passive, pointing to a lack of knowledge or control of the data which it stores" (§ 114 of the decision). Whilst the "neutrality" of the service, on which the responsibility of ISPs depends, is legally recast by the evolution of automated systems for the processing and filtering of huge amounts of data through search engines, data mining, or cloud computing, it is thus an open question whether today's clauses of immunity should protect gigantic information distributors that either control the architecture of the system with its apps or determine control over content of the communication. Reflect on Apple's model of services with more than 350.000 apps only for i-Phones, or Facebook's terms of service, so that the ISP has the right to unilaterally disconnect user groups or block discussion pages. Unsurprisingly, "a trend can be detected in Europe towards reducing the scope of immunities" and enrolling "the ISPs as policemen of their users' activities" (Reed 2012, pp. 63, 61). This trend is confirmed by the provisions of the UK DEA mentioned above in Section 4 and further cases as *Google v. Copiepress* in Belgium, *Vuitton v. eBay* in France, and so forth.

The other side of this trend is represented by today's debate on whether individuals should have the right to access the net. Significantly, one of the main legal issues has to do with the legitimacy of some provisions, such as the French HADOPI law, according to which ISP should be enrolled as sheriffs of the web. Although the French Constitutional Council declared access to the internet to be a basic human right in June 2009, the law finally passed by the French Parliament on 22 October 2009 establishes that internet users ought to be logged off after three notices of copyright infringement. Much as the South Korean variant of the "three strikes" doctrine, or the aforementioned UK DEA from 2010, the provisions of the French law bring us back to the different points of view of the EU Court of Justice and the Court of Appeals in London, as seen above in the previous section. In addition to what type of filtering system should be reckoned as legitimate in the EU law, a further set of problems remain open: Does the individual right to access to the net represent a basic Lockean right (Section 2), thus incompatible with the use of either alleged self-enforcing technologies (Section 3), or omnipresent forms of filtering (Section 4)? Should this new right be balanced against the need of guaranteeing online security? Moreover, how should this balancing work between zero-sum games and win–win approaches (Section 5)? Would it be enough four, or five, strikes? Would not it represent the Western way to a system of filters and re-routers, detours and dead ends, to keep internet users on the state-approved online path, much as in China?

Remarkably, the new *Police and Criminal Justice Data Protection Directive* that the European Commission presented in January 2012 illustrates a feasible way out. Articles 19(2) and 38 of the Proposal mention the principle of privacy by design (and by default), that is, one of the win–win approaches mentioned above in Section 4. In the wording of the Commission, "the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken to ensure that the requirements of the Directive are met. In order to ensure compliance with the provisions adopted pursuant to this Directive, the controller

should adopt policies and implement appropriate measures, which meet in particular the principles of data protection by design and data protection by default" (*op. cit.*, n. 38). As seen above in Section 5, however, this win–win approach has its limits, and this is why the protection of relative (as opposed to absolute) civil rights, at times, has to be balanced against the need of guaranteeing collective and individual security. Going back to the proposed new *Police and Criminal Justice Data Protection Directive*, the EU Commission significantly refers to "the level of protection of the rights and freedoms of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties" which "must be equivalent in all Member States" (Seventh Considerandum of the proposed directive). Moreover, the new *Police and Criminal Justice Data Protection Directive* is rooted in the balancing of the principles of subsidiarity and proportionality, according to Article 16 of the Treaty on the Functioning of the European Union. This means that any intervention envisaged by the directive should not go beyond what is strictly necessary to achieve its objectives and cannot be achieved sufficiently by the Member States but, rather, by reason of the scale or effects of the proposed action, the proper balance between security and civil rights can be better struck by the Union.

Let aside whether the directive will strike such a balance, we should not miss a crucial point: against the "security first" thesis and a number of national statutes, or international attempts to implement a zero-sum game in the field of online security, the proposed directive illustrates how a win–win solution or, at least, a more properly balanced approach is technically feasible. In light of this polarization, the time is ripe for the conclusions of this paper.

7 Conclusions

This paper has dwelt on three possible outcomes of today's debate on online security and civil rights, that is, the opposite views that deem as unnecessary any trade-off between such rights and interests in the name of the "security first" and "liberty first" theses on the political foundations of legal interaction and the idea endorsed by scholars and legislative drafts, or statutes, that aim to strike a proper balance in such fields as constitutional law, international and transnational law, etc. This bifurcation has been traced back to the alternative ways in which the connection between online security *and* civil rights is understood, namely, grasping that "and" in either a disjunctive or a conjunctive way. On one side, focus was on a Hobbesian approach to issues of national, or public, security (Section 2), the use of self-enforcement technologies (Section 3), and systems of filtering on the internet (Section 4), all of which end up with a zero-sum game (Section 5). On the other side, attention was drawn to the protection of absolute civil rights (Section 2), collaborative private interaction (Section 3), and relative basic rights (Section 4) that may entail a win–win scenario (Section 5). These opposite sides of the debate were represented as the ends of a spectrum, within which matters of legal balancing and trade-offs between online security and civil rights are under scrutiny.

More particularly, the paper insisted on how different types of legal interaction, that is, public *and* private (Section 2), *between* private individuals (Section 3), and

within public/private architectures (Section 4), reverberate on the ways in which different types of rights and interests are balanced (Section 5). So, in political interaction, the issue revolves around how to balance national security and human rights in international law, much as national security and fundamental, or civil, rights in constitutional law, whereas such individual rights should be considered as relative, rather than absolute (human, or civil, or fundamental) rights. Then, in social interaction between private individuals, the constitutional right to security has to be balanced with further individual rights, including self-defence and safety. Here, some striking differences of constitutional law have been stressed between the US and EU legal systems, e.g. data protection vis-à-vis the protection of copyright interests. Next, in social interaction within public/private architectures, the balance that should be struck between fundamental, or civil, or human rights, such as the right to privacy, freedom of speech and of information, or the right to conduct a business, has to do with the conditions that make the use of self-enforcing technologies and systems of filtering on the internet legitimate. Accordingly, most of the debate on security and civil rights insists on matters of legal balance, in accordance with two different points. First, this balance pivots around such notions as the principle of proportionality, predictability, or necessity, which are at work with the logic of good more, or less, between different rights and interests in the legal system. Second, as a matter of comparative law, attention should be drawn to the differences between the fields of international and transnational law, much as the different traditions of national legal systems, e.g. the US constitutional right to privacy vs. the EU fundamental right to data protection.

In light of this latter debate, however, a final point should be stressed: over the past years, a number of laws, such as HADOPI or DEA, and legislative drafts, such as ACTA, have aimed to impose zero-sum games. Against this trend, the paper has illustrated three reasons why this approach to issues of online security and civil rights is, at its best, highly problematical and, even, illegitimate, vis-à-vis some case law of the European Court of Human Rights and the EU Court of Justice. First, consider the protection of absolute civil rights, collaborative private interaction, and the protection of relative civil rights that do not admit balancing, e.g. the EU Court of Justice's decisions in *Scarlet* and *SABAM v. Netlog*. Contrary to the logic of good more or less, so as to balance the protection of different rights and interests, what these cases pinpoint is the legal interaction where trade-offs are unnecessary, or illegitimate and, moreover, such legal interaction can be fostered through win–win approaches: contemplate the "appropriate technical and organizational measures" mentioned by the Commission in the proposed new *Police and Criminal Justice Data Protection Directive*. Second, the use of self-enforcing technologies and filtering systems on the internet should be considered as the exception, or last resort option, to guarantee online security and, even in this case, such a use should be strictly balanced against the protection of basic civil rights, e.g. freedom of information. Third, the level of protection concerning such rights, as the right to online access, privacy and data protection, freedom of speech and to conduct a business, may entail no balance under certain circumstances. Therefore, the connection between security and civil rights can either be understood conjunctively, in a win–win scenario, or disjunctively: even in this latter case, however, either civil rights prevail over security (no balancing), or such balance has to satisfactorily protect individual rights (proportionality). At least in Western legal systems, it should be clear that no room is left for zero-sum games in the field of online security.

References

Burns, A., McDermid, J., & Dobson, J. (1992). On the meaning of safety and security. *The Computer Journal, 35*(1), 3–15.

Cavoukian, A. (2010). Privacy by design: the definitive workshop. *Identity in the Information Society, 3*(2), 247–251.

Dworkin, R. (1985). *A matter of principle*. Oxford: Oxford University Press.

Etzioni, A. (2007). *Security first: for a muscular, moral foreign policy*. New Haven: Yale University Press.

Habermas, J. (1996). *Between facts and norms*. Cambridge: Polity Press.

Hobbes, T. (1999). In R. Tuck (Ed.), *Leviathan*. Cambridge: Cambridge University Press.

Jobs, S. (2007). Thoughts on music. http://www.apple.com/hotnews/thoughtsonmusic/. Accessed 22 August 2012

Lessig, L. (2004). *Free culture: the nature and future of creativity*. New York: Penguin.

Locke, J. (1988). In P. Laslett (Ed.), *Two treatises of government*. Cambridge: Cambridge University Press.

Pagallo, U. (2008). *La tutela della privacy negli Stati Uniti d'America e in Europa*. Milano: Giuffrè.

Pagallo, U. (2012a). Cracking down on autonomy: three challenges to design in IT law. *Ethics and Information Technology, 14*(4), 319–328.

Pagallo, U. (2012b). On the principle of privacy by design and its limits: technology, ethics, and the rule of law. In S. Gutwirth, R. Leenes, P. De Hert, & Y. Poullet (Eds.), *European data protection: in good health? 331–346*. Dordrecht: Springer.

Reed, C. (2012). *Making laws for cyberspace*. Oxford: Oxford University Press.

Strauss, L. (1936). *The political philosophy of Hobbes. Its basis and its genesis*. Oxford: Oxford University Press.

Yeung, K. (2007). Towards an understanding of regulation by design. In R. Brownsword & K. Yeung (Eds.), *Regulating technologies: legal futures, regulatory frames and technological fixes* (pp. 79–108). London: Hart.

Zittrain, J. (2007). Perfect enforcement on tomorrow's internet. In R. Brownsword & K. Yeung (Eds.), *Regulating technologies: legal futures, regulatory frames and technological fixes* (pp. 125–156). London: Hart.