*Maria Grazia Porcedda*

# Lessons from PRISM and Tempora: the self-contradictory nature of the fight against cyberspace crimes. Deep packet inspection as a case study

## *A. Introduction*

The leaks about the Tempora[1] and Prism[2] programmes, conducted by the UK and US government respectively, sparked a public outcry[3] that resumed the 'security vs. privacy' debate[4] and underlined the importance of the fundamental rights[5] to (informational) privacy and data protection to democracy.[6]

Surprisingly, however, the potential for policy discussions deriving from the (albeit scant) information on the technology used to perpetrate surveillance was not fully harnessed. Tempora allows "the GCHQ (…) to tap into and store huge volumes of data drawn from fibre-optic [transatlantic] cables for up to 30 days so that it can be sifted and analysed"[7] for information relevant to "security, terror, organised crime…and economic well-being".[8] The National Security Agency (hereafter NSA)'s Xkeyscore allows "real-time interception of an individual's Internet activity",[9] e.g. based on "name, telephone number, IP address, keywords". These accounts hint at the use of deep packet inspection (hereafter DPI), even when the target is traffic data, or data stored by private companies,[10] since Internet Service Providers (Internet access providers, hereafter ISPs) "could reroute the traffic through an encrypted IPsec VPN installed to enable security agencies to have direct access to the [email messages] sent there."[11]

The first policy inference that can be drawn is that PRISM and Tempora are old wine in new bottles. Last year, the UK government proposed a programme compelling ISPs

1 *Macaskill* et al., The Guardian, 21 June 2013.
2 *Gellman / Poitras*, Washington Post, 6 June 2013; *Greenwald / Ball*, ibid.20 June 2013.
3 *Donohue*, The Washington Post, 21 June 2013; European Digital Rights (Edri), EDRI-gram newsletter, 19 June 2013.
4 *Ashworth* 2007, 203-26; *Lepore*, The New York Times, 24 June 2013.
5 'Charter of Fundamental Rights of the European Union (EUCFR)', OJ C 303/1, 14 December 2007, p. 1–22.
6 *Lillington*, Irishtimes.com, 19 June 2013.
7 *Macaskill et al.*, The Guardian, 21 June 2013.
8 Ibid.
9 *Greenwald*, The Guardian, 31 July 2013; *Gallagher*,Ars Technica, 9 August 2013.
10 *Greenwald/Ewen Macaskill*, The Guardian, 7 June 2013.
11 ULD, 'Report on Surveillance Technology and Privacy Enhancing Design', (2013) at 44.

to give security services real-time access to Internet usage data collected through DPI.[12] In 2006, it emerged that the NSA was stealthily wiretapping all traffic passing through a major AT&T switching facility using the Narus Semantic Analyser, a DPI engine.[13] The surreptitious cooperation between the NSA and Google has been suspected for some years.[14]

The second, and crucial, policy inference is that using DPI to sieve the cyberspace for deviant behaviour represents a contradictory and reckless approach to the policy goal of 'cybersecurity'. Moreover, cybersecurity and the safeguard of the privacy and personal data of citizens are inextricably interlinked.

This article looks into such overlooked policy lessons,[15] providing an appraisal, from a EU legal perspective, of the uses of DPI for preventive policing. It does so by first shedding light on the complex scenario of cybersecurity from a legal perspective, which highlights the relation between cybersecurity and the protection of personal data vis-à-vis the policing of deviance. It then reviews the legality of security-related uses of DPI,[16] and appraises them against the issues raised in terms of cybersecurity and data protection.

### *B. The law of cybersecurity: a patchwork of data protection, telecom and NIS laws*

In the EU, cybersecurity is informally defined as the protection of the *cyber domain*, consisting in preserving "the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein."[17] The 'cyber domain' can be seen as comprising four building blocks, which are targeted by law in a piecemeal fashion.

#### I. The networks

The physical networks are made of communication channels (physical cables, radio waves etc.) and routers. The law protects them as critical information infrastructure (CII): fundamental resources and services whose intentional or accidental collapse could seriously endanger the functioning of society.[18] The many ISPs[19] that manage the subnet-

12 *Solon*, Wired, 4 and 18 April 2012.
13 *Landau* 2010; *Poe* 2006.
14 *Kravets*, 11 May 2012; *Porcedda* 2011; *Sommer / Brown* 2011.
15 *Greenwald et al.,* The Guardian, 12 July 2013.
16 See also *Porcedda / Vermeulen / Scheinin* 2013.
17 European Commission and High Representative, 'JOIN (2013) 01 final', (Brussels) at 3, note 3.
18 'CII Directive', OJ L 345, 23 December 2008, p. 75-82; European Commission, COM (2005) 576 Final, (Brussels, 2005); European Commission, COM (2006) 0786, (Brussels, 2006).
19 *Tanenbaum / Wetherall* 2011.

works making up the Internet must also adopt appropriate security measures, as provided for by the Framework[20] and E-privacy[21] Directives.

## II. The Internet architecture

The Internet architecture gives 'cleverness' to the channels and is made of protocol stacks and layering,[22] which: a) transmit bits across the communication channels (physical); b) present the raw transmission as a dedicated, flawless connection (link); c) take care of the communication between sender/recipient through routing (network); d) divide the message into packets and number them (transport); and e) provide protocols for the front-end services, e.g. HTTP for the Web (application, commonly referred to as the content layer).[23]

At first, since Internet users were known and easily sanctionable for misbehaviour, the main architectural concern was reliability rather than security.[24] Civil and criminal law instruments apply indirectly to the architecture, as they primarily concern the function it performs: transporting (data containing) information.

## III. The data transported

Data are transported by packets in accordance with the principle of net neutrality, whereby delivery follows best effort regardless of the content carried. Since data flow from equipment ultimately operated by persons, most of the information carried in the form of content, traffic or location data can (in)directly identify individuals. Thus, the information constitutes personal data in the sense of the Data Protection Directive,[25] protected by the Charter of Fundamental Rights of the European Union (hereafter EU-CFR), like the right to privacy,[26] which is called into question when data reveal details about users' private life. The security of routed data is the overlapping objective of data protection[27], telecom regulation[28] and network and information security (hereafter NIS),[29] blended in the old Commission's 'three-pronged approach'.[30]

Protection is expressed in terms of the classical canons of information security, applied to "stored or transmitted data or the related services offered by or accessible via that

20 'Framework Directive', OJ L 108, 24 April 2002, p. 33–50.
21 'E-privacy Directive', OJ L 201, 31 July 2002, p. 37-47.
22 The most well-known systems of reference are the Open System Interconnection (OSI) and the Transmission Control Protocol/Internet Protocol (TCP/IP).
23 *Tanenbaum / Wetherall* 2011.
24 Ibid.
25 Article 2, 'Data Protection Directive', OJ L 281, 23 November 1995, p. 31-50.
26 Article 8 and 7 EUCFR respectively. For a discussion of these rights, see at *Kreissl et al.* 2013; *Porcedda / Vermeulen / Scheinin* 2013.
27 E-privacy Directive.
28 Framework Directive.
29 European Commission, (Proposed NIS Directive), COM (2013) 48 Final, (Brussels, 2013).
30 European Commission, COM (2001) 298', (Brussels, 2001).

network and information system":[31] i) availability (services are operational as expected); ii) authenticity (users' claimed identity can be established); iii), integrity (transmitted/stored data are unchanged and complete); and iv) confidentiality (unauthorized parties cannot intercept communications/read stored data). The seminal judgment of the Bundesverfassungsgericht[32] makes the well-rooted[33] interconnection between computing, data protection and informational privacy, explicit.

The applicable instruments both require adopting technical tools to block the packets before they jeopardize information security canons, and attempt to thwart the economic incentives to cybercrime.[34] In this sense, they are preventive: if packets do not infect terminal equipment, the threat is avoided.

## IV. The end-point terminal equipment and users

According to the end-to-end principle, communication channels are 'dumb' links connecting 'clever' machines or terminal equipment (e.g. routers, PCs, mobile devices, sensors, RFID-enabled objects, etc.). 'Cleverness' means making the data transmitted intelligible, and this is why the machines are both the targets and the instruments used to perpetrate attacks. A fifth building block of the cyber domain could be humans, who ultimately control the devices: they are behind communications, the adoption of security and the perpetration of crimes. Indeed, the law targets the consequence of humans' actions and behaviours.

## V. The problem of network security

The myriad devices connected to the Internet underscores its value.[35] Unfortunately, calculating the cost of the insecurity of the networks is hindered by technical complexity. A proxy is the rough calculation of the cost of cyberspace crimes,[36] which appears sufficiently high to justify a reactive, rather than preventive approach.[37]

In the EU, cybercrime informally "refers to (…) different criminal activities where computers and information systems are involved either as a primary tool or as a primary target."[38] Wall's 'Internet test'[39] helps distinguishing between different types of cyberspace crimes, which is crucial to appraise the impact of the uses of DPI on data pro-

31 Article 2 of the Proposed NIS Directive.
32 Bundesverfassungsgericht (2008),1 BvR 2074/05 and 1 BvR 1254/07.
33 *Bennett / Raab* 2006; *Rodotà* 1973.
34 See, among others, *Anderson / Moore* 2006; *Porcedda* 2012, 90; Sommer / Brown 2011.
35 This is calculated through Metcalfe's law as the square of the number of its potential connections, equalling the number of connected users, *Tanenbaum / Wetherall* 2011.
36 *Kshetri* 2010.
37 *Anderson et al.* 2012.
38 European Commission and High Representative of the European Union for Foreign Affairs and Security Policy (2013) at 3, note 4.
39 *Wall* 2011; see also *Porcedda* 2012.

tection, privacy and NIS. Some offences are proper cyberspace crimes, in that they would not exist without the Internet. They are the crimes against the data, the logical highway, and the machine, the failure of *cybersecurity* that result from harming the information security canons. Investigating such failures clashes against the conundrum of attribution: the difficulty in tracing the machine initiating a crime, and the individual behind it.[40] The revised Directive on Attacks against Information Systems,[41] and articles 2-6 of the Convention on Cybercrime (hereafter the Convention),[42] criminalize the following: illegal access (hacking); illegal interception (breach of confidentiality); system interference (denial of service attacks, spam); data interference (malware); and misuse of devices (production and sale of harmful software and devices). The Convention, and the policy discourse, cover also offences that exist before and outside the Internet: data revealing lawbreaking information, material covered by copyright and intellectual property, material offending morals, such as expressions of hatred, and child pornography.

***

Setting aside the problem of attribution, the Convention lays down common rules for investigating all types of crimes (beyond those listed) occurring in cyberspace, and urges the adoption of tools enabling to intercept and access information. Existing tools, often stemming from the private sector, permit to detect and block the packets so that the offensive content is not spread further, and support investigation for *both* types of crimes. These include[43] live interception of data through DPI, analysed in the following in its applied uses[44] from a legal and NIS perspective.

### *C. DPI: features and uses*

DPI is a technology, placed in routers, empowering ISPs to screen 'live' all packet layers (including the payload, i.e. content) sent over the networks, thus challenging the end-to-end principle. Mueller defines DPI an "enabling technology",[45] in that its functioning depends on the applications or modules installed: recognition, notification and manipulation. Recognition uses data mining algorithms to analyse, on- and offline, any parts

40 *Landau* 2010.

41 European Commission, COM (2010) 517, (Brussels, 2010), revising 'Council Framework Decision on Attacks against Information Systems', OJ L 69, OJ L 69, 16 March 2005, p. 67-71.

42 Council of Europe, 'Convention on Cybercrime', CETS n° 105 (Budapest, 2001).

43 Also, data analysis techniques, such as open data mining for profiles or social network analysis; filtering and blocking content (*Anderson / Murdoch* 2008; *Mcintyre* 2011.); and the use of state-sponsored malware to intrude in systems and intercept communications.

44 For calls for an analysis of DPI in context, see Office of the Privacy Commissioner of Canada, Collection of essays on DPI, available at: http://www.priv.gc.ca/information/research-recherche/dpi_intro_e.asp.

45 *Mueller* 2011 at 2. On the subject, see also *Bendrath / Mueller* 2010; *Del Sesto / Frankel* 2008; *Berners-Lee* 2009; *Bendrath* 2009; *Daly*,2010; *Ohm* 2008.

of the packets at any layer of the Internet architecture against specific patterns or features (keywords contained in a predefined library), and compares the obtained data on the basis of such patterns and keywords. Notification consists in sending alerts in relation to the patterns and keywords identified, and is usually conducted offline. DPI engines combining recognition and notification are called 'passive'. Manipulation, or 'active' DPI, affects the destination of the packets and can be performed both on- and offline.

DPI evolved from shallow and meso-packet inspection tools, and started being distributed a decade ago to detect and prevent malware[46], which is of obvious import for cybersecurity. Yet, its potential for eavesdropping was soon apparent: DPI seemed suitable to fulfil the legal requirements of the US Communications Assistance for Law Enforcement Act (CALEA), whereby all ISPs must install any available technologies enabling lawful wiretapping.[47] Either with a view to recover the investment,[48] or pushed by 'Google envy',[49] companies started using it for lucrative services such as ad-injection (the evolution of behavioural advertising[50]) and 'network management'[51] (traffic prioritization). In turn, organizations interested in the protection of digital rights lobbied for its use, and it was soon apparent that DPI could be used for policing the networks from all sorts of content deemed unlawful: material offending the (culture-sensitive) definition of morals[52], such as pornography; the expression of hatred; child pornography; or material consisting in (regime-sensitive) subversive speech. In other words, DPI represented a new and powerful means for old ends.[53]

### *D. Appraising the uses of DPI for 'security' purposes from a legal perspective: the test of privacy and data protection*

The packets screened by DPI carry data produced in the course of "personal Internet usage"[54] and communications (e.g. e-mails or Voice over Internet Protocol, VOIP), which contain information susceptible to identifying an individual. Hence, their collection represents an intrusion into the right to personal data protection.[55] Moreover, "personal Internet usage" and communications fall within the broad definition of correspondence ("communication" in the language of the EUCFR), [56] an attribute of the right to

46 *Bendrath* 2009.
47 *Ohm* 2008; *Landau* 2010.
48 *Landau* 2010.
49 *Ohm* 2008.
50 *Bendrath* 2009.
51 Network management could be defined as the "activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems." *Ohm* 2008 at 51.
52 *Akdeniz* 2011.
53 *Bendrath* 2009.
54 Copland v. The United Kingdom, n. 62617/00, ECtHR, at § 41.
55 Article 8 EUCFR. C-360/10, Belgische Vereniging Van Auteurs, Componisten En Uitgevers Cvba (Sabam) v Netlog Nv, CJEU, at § 45.
56 Copland v. The United Kingdom, at § 41.

privacy (to be interpreted in line with the case law relating to article 8 of the European Convention of Human Rights[57], hereafter ECHR). The monitoring of information produced in the course of correspondence, including traffic and location data,[58] constitutes an interference with the right to private life irrespective of whether the correspondence is private.[59] Furthermore, individuals have a reasonable expectation of privacy if there is no warning about the monitoring of 'correspondence'.[60]

Since DPI is susceptible of intruding into the rights to privacy and data protection, its uses are only admissible if they fully comply with a test for permissible limitations.[61] First, the intrusion must be "in accordance with the law" or "provided for by the law":[62] there must be a domestic legal basis respecting set standards of quality.[63] Second, intrusions must respect the essence of the rights to privacy and data protection. This is a contentious matter in legal scholarship, and current studies are exploring methodologies;[64] a possible approach is to look at rights in terms of their attributes and carry out a legal assessment accordingly.[65] Third, intrusions must be necessary in a democratic society, which implies that "the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued"[66] (subject to states' margin of appreciation). Legitimate aims in the EU are either the objectives of general interests enshrined in article 3 of the Treaty on the European Union, or the protection of the rights and freedoms of other. These include serious crime and the protection of national security.

Article 21 of the Cybercrime Convention contains a legal basis potentially allowing the use of DPI: states can enable 'service providers', for the sake of serious offences, to conduct real-time (confidential) interception ('collection or recording') of content data, relating to specified communications transmitted by means of a computer system.

Ad-injection, copyright infringement and network management do not have any security import, and they would thus not pass one or more parts of the permissible limi-

57 Council of Europe, 'Convention for the Protection of Human Rights and Fundamental Freedoms', CETS n° 005, 4 November 1950 (Rome).
58 Copland v. The United Kingdom, at § 43.
59 Niemietz v.Germany, n. 13710/8, ECtHR, at § 32.
60 Copland v. The United Kingdom, at § 42.
61 See *Porcedda / Vermeulen / Scheinin* 2013.
62 Articles 8.2 ECHR and 52.1 EUFCR respectively.
63 See, inter alia, Shimovolos V. Russia, n. 30194/09, ECtHR, at § 67. The law must be accessible and respect the rule of law (Rotaru v. Romania, n. 28341/95, ECtHR, at § 59). When they do not establish secret measures of surveillance, laws must enable individuals to foresee (Shimovolos v. Russia, at § 68), if need be with appropriate advice, with sufficient precision the consequences produced upon them and thus regulate their conduct.
64 For a discussion on the subject, see *Kreissl et al.* 2013.
65 *Porcedda* 2013. However, since the method is still experimental, it is not going to be tested here.
66 Leander v. Sweden, n. 9248/81, ECtHR, at §§ 58-59. Article 52§ 1 EUCFR.

tations test, as compellingly demonstrated elsewhere.[67] In the following, the reasoning is applied to malware and spam detection, content control and eavesdropping.

## I. Malware and spam

Both malware and spam are cybercrimes and serious offences. Malware is considered 'illegal data interference',[68] which compromises the integrity, availability and confidentiality of data stored in the terminal equipment of both single and multiple users, or devices (when servers or unprotected cloud data centres are infected). Depending on the device attacked, malware can affect CII,[69] industrial secrets, and obviously users' rights to data protection and confidentiality of communications. Spam is prohibited by the E-privacy Directive[70] and constitutes illegal system interference[71] affecting the availability of systems, which is a legal interest of operators and users.

The E-privacy and Framework Directives[72] oblige electronic communications services and network providers to employ suitable technical and procedural means to ensure the security of the network and the services issued therein. These instruments thus offer a preliminary legal basis for the adoption of malware-oriented DPI, as recognized by the EDPS,[73] and the Article 29 Data Protection Working Party[74] (in the context of email services).

Since malware-oriented DPI can block threats before they spread, it both prevents crime and protects personal data and the confidentiality of communications. These are legitimate aims that allow an interference with both the right to private life and data protection;[75] moreover, the interference aims at better protecting the restricted rights. This use would thus be permissible, with some qualifications expressed in the conclusions.

## II. Child pornography as an example of content control

Child pornography is a discomforting topic, as it concerns the most vulnerable members of society, and the citizens of the future. Unsurprisingly, it is an emotionally charged, and at times biased, subject. This makes it an imperative case study of content control, because protection of children is a legitimate aim necessary in a democratic society. The

67 In general, see EDPS, 'Opinion on Net Neutrality, Traffic Management and the Protection of Privacy and Personal Data', Brussles, (2011). For the use of DPI for ad-injection, see *Kuehn / Mueller* 2012. For the case of network management, see *Ohm* 2008; for copyright infringment, see C-360/10, Sabam v. Netlog Nv, CJEU.
68 Convention, article 4.
69 As the cases of Stuxnet, Duqu and Flame malware showed.
70 Article 12.
71 Convention, article 5.
72 Articles 4.1, and articles 13 letters a) and b) respectively.
73 EDPS 2011.
74 Article 29 Data Protection Working Party, 'Opinion 2/2006'. WP 118', Brussels, (2006).
75 Niemietz v.Germany, at § 36.

subject has been widely studied elsewhere,[76] and here I only focus on the permissibility of DPI in relation to it.

Child pornography does not concern cybersecurity; rather, it is a horrific activity and a business pursued by organized crime online.[77] It is considered an offence by both the Convention[78] and the anti-Child Abuse Directive,[79] and subsumes three meanings: a) pseudo child pornography, i.e. images portraying seemingly underage adults (18+) in pornographic poses; b) synthetic child pornography, i.e. the manipulation of pictures of children to simulate scenes of abuse; c) real child pornography, that is the portrayal of an act of abuse on a child.

DPI is said to be a very useful tool to uncover cases of child abuse and pornography and take down rings of (gainful) abusers. Buttressing such claims is fundamental for assessing the proportionality of the measure, but in order to appraise permissibility, I should start with legality. To date, there is no legal basis authorizing the use of DPI engines for the detection of child pornography. The anti-Child Abuse Directive provides a legal basis for blocking and taking down content akin to child pornography,[80] but it does not lay down rules (on methods) for detecting pornographic material. The recent trend in drafting memoranda of understanding between police services and private actors with a view to "identifying and removing known child pornography material" and "increasing as much as possible the volume of system data examined,"[81] offers an invalid solution. Memoranda of understanding do not have the force of law. The legal basis authorizing the use of DPI engines for the detection of child pornography must be adopted at the EU level, as not to do so would hinder the competitive development of the internal market.[82]

Moreover, requiring service providers to run DPI engines would infringe the prohibition of general monitoring laid down by the e-Commerce Directive,[83] whereby member states must not oblige ISPs "to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity", as reminded by the Court of Justice of the European Union in the *Scarlet extended* and *Netlog* cases.[84]

Hence, the use of DPI in case of investigations relating to child pornography is currently impermissible. Yet, should such a legal basis be introduced, it would be likely to pass the proportionality test only in the case of real pornography.[85] It should also be noted that DPI could do nothing to prevent abuse *per se*, but simply block the circulation

76 *Mcintyre* 2011.
77 *Sommer / Brown* 2011.
78 Convention, article 10.
79 Article 2 of 'Directive 2011/92/EU,' OJ L 335, 17 December 2011 p. 1-14.
80 Article 25.
81 Global Alliance Partners 2012.
82 C-301/06, Ireland v. European Parliament and Council, CJEU.
83 OJ L 178, 17 July 2000, p. 1-16, article 15(1).
84 Sabam v. Netlog.
85 Unfortunately, it is not possible to comment the matter further here. As a reference, see the *Akdeniz* 2011. See also Perrin v. The United Kindgom n. 22594/93, ECtHR.

of pictures, and, in an unknown percentage of cases, lead to identification and prosecution of perpetrators. This raises serious issues of public policy and proportionality, as addressed in the conclusion.

1. Eavesdropping for serious crime and national security

The Tempora and PRISM programmes offer a clear example of the use of DPI[86] engines to tackle national security and serious crime at large, such as terrorism[87]and all threats, unrelated to NIS, posed by 'deviant behaviour'.

The Convention[88] allows extending the scope of application of real-time interception of content data[89] to "Other criminal offences committed by means of a computer system, and the collection of evidence in electronic form of a criminal offence," such as 'online terrorism'. Existing legal provisions either allow wiretapping specific individuals, or mandate the retention of telecoms data for the purposes of investigating serious crime. Not only the Data Retention Directive[90] does prohibit retaining content data, which violates the confidentiality of communications, but also it mandates that "data retained in accordance with this Directive are provided only to the competent national authorities in *specific cases* and *in accordance with national law*".[91]

The reasoning behind the inadmissibility of DPI for child pornography applies, *mutatis mutandis*, to eavesdropping and fishing expeditions. National provisions should stem directly from – currently absent – EU provisions, which should solve the conundrum of the prohibition of general monitoring by ISPs first.[92] Hence, using DPI engines for fishing expeditions is impermissible as it lacks a legal basis and infringes existing applicable law.

*E. Appraising the uses of DPI from a cybersecurity perspective*

According to its informal definition, cybersecurity does not aim at policing the Internet from traditional deviance, but at preserving the classical information security canons. Generic online (passive or active) *unauthorized* DPI could amount to illegal interception,[93] i.e. the loss of confidentiality of personal data. Active DPI could also amount to system interference,[94] which is the serious hindering of the availability of a computer

86 *Latif*, The Inquirer.net 5 December 2012.
87 United Nations Office on Drug and Crime (Unodc), 'The Use of Internet for Terrorist Purposes', Vienna, United Nations (2012).
88 Article 14.
89 Article 21.
90 Combined reading of recital 13, articles 2 and 5.2 of the Data Retention Directive, OJ L 105/54, 13 April 2006, p. 54–63.
91 Article 4.
92 E-commerce Directive, article 15.
93 Convention, article 3.
94 Convention, article 5.

system. Running DPI could thus constitute state-corporate crime, namely "Illegal or socially injurious actions that occur when one or more institutions of political governance pursue a goal in direct co-operation with one or more institutions of economic production and distribution".[95]

Moreover, the short-term advantages for serious crime investigation would severely affect NIS and the rights to privacy and data protection. Landau wrote that the security risks would dwarf the enormous privacy ones.[96]In fact, there would be little incentives to protect the collected information, which could be exploited by both insiders (due to the appeal of big data)[97] and malicious outsiders. After the 2006 AT&T scandal, it emerged that the Narus DPI engine could be configured, once sold, as the users saw fit.[98] Infamously, in the 'Athens Affair' CALEA-compliant software sold by Ericsson to Vodafone Greece was used to intercept the government's communications for almost a year before the 2004 Olympic Games.[99]

The case of malware-oriented DPI is different. Since its final aim is to achieve higher information security, its use should be encouraged,[100] provided it is controlled and audited. In fact, private companies may sell DPI as a malware solution and then use it for other purposes,[101] in particular since their business model and the interest of law enforcement officers tend to meet online.[102]

### *F. Lessons from PRISM and Tempora: avoiding societal collateral damage and cybersecurity risks*

The outcome of the analysis of the legal permissibility of DPI (based on its potential intrusion into the rights to privacy and data protection), and the impact on cybersecurity understood as NIS allows drawing some meaningful conclusions.

The use of spam- and malware-oriented DPI is both permissible and welcome: the intrusion into the two rights is geared to safeguard them, as well as NIS. However, a specific provision concerning DPI's use for malware and spam detection should be adopted to ensure the proportionality (engines should focus on viruses only[103]) and transparency of the tool, and enabling appropriate scrutiny. The use of DPI for content control and eavesdropping is currently impermissible, as it both lacks a legal basis, thus violating the rights to privacy and data protection, and imperils cybersecurity.

Endangering NIS for the sake of short-term investigative advantages is contradictory in two ways. First, because cybersecurity is regarded as a crucial national security matter.

95 *Kramer /. Michalowski / Kauzlarich* 2002 at 270.
96 *Landau* 2010.
97 *Lanier* 2013.
98 *Poe* 2006.
99 *Landau* 2010.
100 Currently its use is limited, as ISPs can outsource Internet security to users. *Bendrath* 2009.
101 *Landau* 2010.
102 *Schneier* 2013.
103 EDPS 2011.

The use of DPI engines is not the only example of contradiction[104]: the use of state-sponsored malware is another case in point (e.g. the 'Magic Lantern' and the Bundestrojaner).[105] Second, because affecting the confidentiality of communications exposes to the danger of 'societal collateral damage': harming the very rights and privileges that characterise our democracy[106] and that we cherish.

The European Court of Human Rights acknowledged that a "system of secret surveillance for the protection of national security poses the risk of undermining or even destroying democracy on the ground of defending it." [107] DPI can be used only if auditable and subject to strict (judicial) control, which is difficult as ISPs run the engines. Moreover, asking ISPs to run DPI engines constitutes a form of 'tilting',[108] whereby private actors would perform the role of police services, amassing detailed profiles of citizens without being submitted to the same judicial scrutiny: "DPI is a letter carrier who reads all your mail, listens to all your calls, follows you as you browse downtown and in the mall, notes your purchases, listens in as you ask questions of the research librarian, and watches over your shoulder as you read the daily paper – and then correlates the information in real time."[109] "The Stasi could only dream of such data."[110]

The ECtHR established that proportionality has to be judged on a case-by-case basis, in relation to the aim pursued.[111] What aim can justify the cooperation of private and state actors for the destruction of the basis of democracy? The reply is none, for the adults of today, and for those of tomorrow.

## Bibliography

*Akdeniz* (2011) Report. Freedom of Expression on the Internet. A study of legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the Internet in OSCE participating States

*Anderson/Moore* (2006) The Economics of Information Security, in: Science, 314 (3), 51

*Anderson/Murdoch* (2008) Tools and Technology of Internet Filtering, in: Palfrey/Deibert/Rohozinski/Zittrain (ed.), Access Denied: The Practice and Policy of Global Internet Filtering

104 See, surprisingly, *Sanger*, New York Times, 12 August 2013. Under Einstein, DPI engines already analyse all traffic passing through US governmental networks for security purposes.
105 *Landau* 2010; *Cluley*, NakedSecurity, 9 October 2011; European Digital Rights (Edri), Edri-Gram Newsletter, N. 10.20', 24 October 2012 and n. 11.12, 19 June 2013.
106 As many authors argue; among those cited in this paper, see *Landau* 2010; *Ohm* 2008; *Rodotà* 1973; and *Bennett / Raab* 2006.
107 Leander v. Sweden at §§ 59-60; Klass v. Germany n. 5029/71, ECtHR, 9 March 1977 at §§ 49-50.
108 *Mcintyre* 2011.
109 *Landau* 2010 at 220, quoting Timothy Garton-Ash.
110 Ibid., at 221.
111 Niemietz v.Germany, at § 37.

*Anderson/Ross et al.* (2012) Measuring the Cost of Cybercrime'. Available at: http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

*Article 29 Data Protection Working Party* (2006) Opinion 2/2006 on privacy issues related to the provision of email screening services. WP 118

*Ashworth* (2007) Security, Terrorism and the Value of Human Rights, in: Goold/Liora (eds.), Security and Human Rights, 203-26

*Bendrath* (2009) Global technology trends and national regulation: Explaining Variation in the Governance of Deep Packet Inspection, in: International Studies Annual Convention

*Bendrath/Mueller* (2010) The End of the Net as we know it? Deep Packet Inspection and Internet Governance. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1653259

*Bennett/Raab* (2006) The Governance of Privacy. Policy Instruments in a Global Perspective

*Berners-Lee* (2009) No Snooping. Available at: http://www.w3.org/DesignIssues/NoSnooping.html

*Bundesverfassungsgericht* (2008),1 BvR 2074/05 and 1 BvR 1254/07

Charter of Fundamental Rights of the European Union (2007), OJ C 303/1, 14 December 2007, 1–22

*Cluley* Government' backdoor R2D2 Trojan discovered by Chaos Computer Club, in: NakedSecurity, 9 October 2011

Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems', OJ L 69, 16 March 2005, 67-71

*Council of Europe* (2001) Convention on Cybercrime, in: CETS n° 105

--- (1950) Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No 11 and 14, in: CETS n° 005

*Court of Justice of the European Union (CJEU)* (2012) Case C360/10, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV

--- (2009) Case C-301/06, Ireland v European Parliament and Council

*Daly* (2010) The legality of deep packet inspection, in: First Interdisciplinary Workshop on Communications Policy and Regulation 'Communications and Competition Law and Policy – Challenges of the New Decade

*Del Sesto/Frankel* (2008) How Deep Packet Inspection Changed the Privacy Debate. Available at: http://dpi.priv.gc.ca/

Directive of the European Parliament and of the Council 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23 November 1995, 31-50

--- 2002/21/EC of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), OJ L 108, 24 April 2002, 33–50

--- 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on e-commerce), OJ L 178, 17 July 2000, 1-16

--- 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (e-Privacy Directive), OJ L 201, 31 July 2002, 37-47

--- 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (Data Retention Directive), OJ L 105/54, 13 April 2006, 54–63

--- 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, OJ L 345, 23 December 2008, 75-82

--- 2011/92/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, OJ L 335, 17 December 2011, 1-14

*Donohue* NSA surveillance may be legal — but it's unconstitutional, in: The Washington Post, 21 June 2013

*European Commission* (2001) Communication on Network and Information Security: Proposal for a European Policy Approach. COM (2001) 298

--- (2005) Green Paper on a European Program for Critical Infrastructure Protection. COM (2005) 576 final

--- (2006) Communication from the Commission on a European Programme for Critical Infrastructure Protection. COM (2006) 0786

--- (2010) Proposal for a Directive on attacks against information systems and repealing Council Framework Decision 2005/222/JHA. COM(2010) 517

--- (2013) Proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union. COM (2013) 48 final

*European Commission and High Representative of the European Union for Foreign Affairs and Security Policy* (2013) Joint Communication EU Cyber Security strategy: An open, safe and secure Cyberspace. JOIN (2013) 01 final

*European Court of Human Rights (ECtHR*) Case of Copland v. the United Kingdom, (n. 62617/00) Judgment of 3 April 2007

--- Case of Klass v. Germany (n. 5029/71), Judgment of 6 September 1968

--- Case of Leander v. Sweden (n. 9248/81), Judgment of 26 March 1987

--- Case of Niemietz v.Germany (n. 13710/88 ), Judgment of 16 December 1992

--- Case of Perrin v. the United Kindgom (22594/93), Judgment of 18 October 2005

--- Case of Rotaru v. Romania (28341/95), Judgment of 4 May 2000

--- Case of Shimovolos v. Russia (n. 30194/09), Judgment of 21 June 2011

*European Data Protection Supervisor (EDP*S) (2011) Opinion on Net Neutrality, Traffic Management and the Protection of Privacy and Personal Data, OJ C 34, 1–17

*European Digital Rights (EDRI)* Details on German State Trojan programme, EDRigram newsletter, n. 10.20, 24 October 2012

--- The Spanish Police might use spying Trojans on individuals' computers, EDRI-gram newsletter, n. 11.12, 19 June 2013

--- US agencies have unlimited access to Internet data, EDRI-gram newsletter, n. 11.12, 19 June 2013

*Gallagher* Building a panopticon: the evolution of the NSA's XKeyscore, in: Ars Technica, 9 August 2013

*Gellman/Poitras* NSA slides explain the PRISM data-collection program, in: Washington Post, 6 June 2013

*Global Alliance Partners* (2012) Guiding principles on the Global Alliance against child sexual abuse online. Annex to the Declaration on Launching the Global Alliance against child sexual abuse online. Available at: http://ec.europa.eu/dgs/home-affairs/what-is-new/news/news/2012/docs/20121205-declaration-anex_en.pdf

*Greenwald* XKeyscore: NSA tool collects 'nearly everything a user does on the internet, in: The Guardian, 31 July 2013

*Greenwald/MacAskill* NSA taps into systems of Google, Facebook, Apple and others, secret files reveal, in: The Guardian, 7 June 2013

*Greenwald/Ball* Revealed: the top secret rules that allow NSA to use US data without a warrant, in: The Guardian, 20 June 2013

*Greenwald et al*. How Microsoft handed the NSA access to encrypted messages, in: The Guardian, 12 July 2013

*Kramer/Michalowski/Kauzlarich* (2002) The origins and development of the concept and theory of state-corporate crime, in: Crime & Delinquency, 48 (2), 263-82

*Kravets* Court Upholds Google-NSA Relationship Secrecy, in: Wired, 11 May 2012

*Kreissl et al.* (2013) SurPRISE Deliverable 3.4 (WP3) 'Exploring the Challenges: Synthesis Report

*Kshetri* (2010) The global Cybercrime Industry. Economic, Institutional and Strategic Perspectives

*Kuehn/Mueller* (2012) Profiling the Profilers: Deep Packet Inspection for Behavioral Advertising in Europe and the United States

*Landau* (2010), Surveillance or Security? The Risk Posed by New Wiretapping Technologies

*Lanier* (2013) Who owns the future?

*Latif* ITU approves deep packet inspection standard behind closed doors, in: The Inquirer.net, 5 December 2012

*Lepore* The PRISM. Privacy in an age of publicity, in: The New Yorker, 24 June 2013

*Lillington* It's good to talk in public about privacy and data protection, in: Irishtimes.com, 19 June 2013

*MacAskill et al*. GCHQ taps fibre-optic cables for secret access to world's communications, in: The Guardian, 21 June 2013

*McIntyre* (2011) Child Abuse and Cleanfeeds: Assessing Internet Blocking Systems. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1893667

*Mueller* (2011) DPI technology from the standpoint of internet governance studies: an introduction (v 1.1)

Ohm (2008) The Rise and Fall of Invasive ISP Surveillance, in: Working Paper n. 8-22

*Poe* The Ultimate Net Monitoring Tool, in: Wired, 17 May 2006

*Porcedda* (2011) Transatlantic Approaches to cyber-security: the EU-US Working Group on Cyber-security and Cybercrime,' in Pawlak (ed.), The EU-US security and justice agenda in action

--- (2012) Data Protection and the Prevention of Cybercrime: the EU as an AREA of Security?, in: EUI Working Paper (Law 2012/25) 90

--- (2013) Paper Establishing Classification of Technologies on the Basis of their Intrusiveness into Fundamental Rights. SURVEILLE deliverable D2.4

*Porcedda/Vermeulen/Scheinin* (2013) Report on regulatory frameworks concerning privacy and the evolution of the norm of the right to privacy. Deliverable 3.2, SurPRISE Project. Forthcoming

*Rodotà* (1973) Elaboratori Elettronici e Controllo Sociale

*Sanger* N.S.A. Leaks Make Plan for Cyberdefense Unlikely, in: New York Times, 12 August 2013

*Schneier* (2013),The Vulnerabilities Market and the Future of Security 2013. Available at: www.schneier.com/crypto-gram-1206.html

*Solon* FAQ: the coalition's email and web surveillance plans explained, in: Wired, 4 April 2012

--- Tim Berners-Lee: deep packet inspection a 'really serious' privacy breach, in: Wired, 18 April 2012

*Sommer/Brown* (2011) Reducing Systemic Cybersecurity Risks. OECD/IFP Project on Future Global Shocks', IFP/WKP/FGS(2011)3. Available at: http://www.oecd.org/governance/risk/46889922.pdf

*Tanenbaum/Wetherall* (2011) Reti di Calcolatori (Quinta Edizione)

*Unabhaengiges Landeszentrum fuer Datenschutz (ULD*) (2013) Report on Surveillance Technology and Privacy Enhancing Design, Deliverable 3.1, SurPRISE Project

*United Nations Office on Drug and Crime (UNODC)* (2012) The Use of Internet for Terrorist Purposes

*Wall* (2011) Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace, in: Police Practice and Research: an International Journal, 8 (2): 183-205

Contact:

*Maria Grazia Porcedda*
*PhD Candidate &*
*Research Assistant to Professor Martin Scheinin*
*Surprise & Surveille FP7 Projects*
*European University Institute*
*Department of Law, Villa Schifanoia*
*Via Boccaccio 121, 50133 Firenze – Italy*
*maria.porcedda@eui.eu*