EJLT European Journal of Law and Technology

Who can protect Network and Information Security? Fixing the Draft ePrivacy Regulation

Andrew Cormack[1]

Abstract: Over the past decade, European law has increasingly recognised the vital role of network and information security in protecting personal data. Most recently the Article 29 Working Party recommended that all data controllers and processors should have processes to detect security breaches. Where personal data are held on networked computers such processes will depend on monitoring logfiles and network traffic. Unfortunately, the European Commission's draft ePrivacy Regulation assumed that this activity is only performed by network operators, raising the possibility that a vital data protection tool will become unlawful for all other organisations. This paper discusses the draft Regulation and amendments proposed by the European Parliament and Council, and suggests how these should be interpreted to still allow online systems and data to be protected.

Keywords: ePrivacy, Data Protection, Information Security, Logfiles

1. Network and Information Security in Data Protection Law

To protect the security of online data, services and users it is essential to know what is happening on the networks and systems that connect them. As Cormack (2016) describes, this is the only way to detect many kinds of attacks and incidents, and to investigate how they can be prevented and remedied. Organised incident response teams have been doing this since at least 1988; the first international meeting of Computer Security Incident Response Teams took place in 1990 (FIRST, 2018a). This CSIRT community now extends to retailers, banks, car and plane manufacturers, providers of computer hardware, software and services, drinks companies, network operators, governments, universities and many others (FIRST, 2018b). Fundamental to the work of all these teams are logfiles containing IP and e-mail addresses, usernames, and other identifiers that European Data Protection law considers to be personal data.

This activity was not mentioned in data protection law until 2009, when Recital 53 of *Directive 2009/136/EC* amended the *ePrivacy Directive (2002/58/EC)* to add:

> The processing of traffic data to the extent strictly necessary for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity

> and confidentiality of stored or transmitted data, and the security of the related services offered by, or accessible via, these networks and systems, by providers of security technologies and services when acting as data controllers is subject to Article 7(f) of Directive 95/46/EC. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.

This recognition of network and information security as a legitimate interest – in the sense of Article 7(f) of the *Data Protection Directive* – appears narrow, being limited to 'providers of security technologies and services when acting as data controllers'. Many organisations that do not provide security technologies or services to others still need to secure their own network-connected systems. However, Article 3 of the *ePrivacy Directive* can be seen as offering a somewhat wider scope: 'This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community', while that Directive's title is still broader: network and information security clearly 'concerns … the protection of privacy in the electronic communications sector'.

Regulators, courts and legislators have, indeed, taken a wide view of the applicability of this Recital, and an even wider one of where network and information security activities should be encouraged. In their 2006 Opinion on Privacy Issues Related to the Provision of Email Screening Services, the Article 29 Working Party of European Data Protection Supervisors presumed without comment that the activities of Email Service Providers (ESPs) – although not considered 'public communications service providers' – did involve 'the processing of personal data in connection with the provision of publicly available communications networks'. The Working Party's analysis therefore referred to the *ePrivacy Directive*, as well as the *Data Protection Directive*. The Working Party considered that 'given that the delivery of emails containing virus may shut down the email service providers system … and thus impair the transmission of further email communications', scanning emails to detect viruses was an acceptable security measure. In addition, 'threats to the general performance of email and network services can justify ISPs and ESPs to engage in filtering for anti-spam purposes'.

In 2016 the European Court of Justice found, in *Breyer v Germany*, that website operators, too, 'may also have a legitimate interest in ensuring, in addition to the specific use of their publicly accessible websites, the continued functioning of those websites' (para 60) and 'the objective aiming to ensure the general operability of those services may justify the use of those [logfiles] after consultation of those websites' (para 64). Finally, also in 2016, Recital 46 of the *Network and Information Security Directive* required all operators of essential services and digital service providers (defined to cover online services whose absence could cause significant damage to critical infrastructures and socially-important services) to take 'measures to identify any risks of incidents, to prevent, detect and handle incidents and to mitigate their impact'. The Commission's draft implementation guidance (2018) requires:

> (a) detection processes and procedures maintained and tested to ensure timely and adequate awareness of anomalous events;
> (b) processes and policies on reporting incidents and identifying weaknesses and vulnerabilities in their information systems;

The NIS Directive also requires public authorities to process personal data for security

purposes: 'competent authorities and data protection authorities should cooperate and exchange information on all relevant matters to tackle any personal data breaches resulting from incidents' (Recital 63).

Recital 49 of the 2016 *General Data Protection Regulation* (GDPR) codified this wider scope: repeating the *ePrivacy Directive*'s permission of '[t]he processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security', and explicitly extending it to cover 'public authorities, … computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), … providers of electronic communications networks and services and … providers of security technologies and services'. The Article 29 Working Party's 2018 guidance on Breach Notification further extended this list to include any organisation that processes personal data:

> Controllers and processors are therefore encouraged to plan in advance and put in place processes to be able to detect and promptly contain a breach, to assess the risk to individuals, and then to determine whether it is necessary to notify the competent supervisory authority, and to communicate the breach to the individuals concerned when necessary (p.6).

This appeared to establish network and information security as a 'technical or organisational measure[]' required of data controllers under Article 17(1) of the *Data Protection Directive* and Article 5(1)(f) of the GDPR. European law therefore seemed clear that a wide variety of organisations were both expected and allowed to process the personal data that was necessary to keep their networks and information secure.

2. Network and Information Security under the draft ePrivacy Regulation

However, this consistent message was contradicted by the draft *ePrivacy Regulation*, published by the European Commission in January 2017. The scope of this Regulation is declared in Article 2(1) to be:

> ... the processing of electronic communications data carried out in connection with the provision and the use of electronic communications services and to information related to the terminal equipment of end-users.

Comparing with the scope of the 2009-amended *ePrivacy Directive,* above, it is apparent that this has been broadened by adding 'the use' of communications services, as well as extended to cover 'information related to the terminal equipment of end-users'. The apparent deletion of the limitation to 'public' communications services is in fact moved to Article 2(2)(c), so this is unchanged.

Adding 'processing … in connection with … the use of electronic communications services' confirms the Article 29 Working Party's presumption that email and similar service providers are included; it also seems hard to argue that any network-connected system that uses its logfiles to detect and investigate security incidents is ***not*** processing 'in connection with … the use of' the networks over which the system is accessed. Indeed, to be effective, the content of the Regulation must apply to all these services and more.

Recital 8, as amended by the European Council on 4th May 2018, attempts to list the organisations to which the various Articles apply:

> ...providers of electronic communications services, … providers of publicly available directories, and ... providers of software permitting electronic communications, including the retrieval and presentation of information on the internet … natural and legal persons who use electronic communications services to send direct marketing commercial communications or make use of processing and storage capabilities of terminal equipment or collect information processed by or emitted by or stored in end-users' terminal equipment.

Thus, even if an online service were somehow outside Article 2(1)'s 'use of' clause, any cookies, fingerprinting or client-side scripts would bring it explicitly within the Regulation's scope.

Unlike the Directive, the Commission's proposed Regulation begins with a general prohibition, in Article 5:

> Electronic communications data shall be confidential. Any interference with electronic communications data, such as by listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance or processing of electronic communications data, by persons other than the end-users, shall be prohibited, except when permitted by this Regulation.

Since neither Articles nor Recitals contain any limitation to this ban, it must apply to all those within the broad scope of the Regulation. The Commission recognised that this would make both operating networks and securing them impossible, so created an exemption in Article 6(1):

> Providers of electronic communications networks and services may process electronic communications data if:
> (a) it is necessary to achieve the transmission of the communication, for the duration necessary for that purpose; or
> (b) it is necessary to maintain or restore the security of electronic communications networks and services, or detect technical faults and/or errors in the transmission of electronic communications, for the duration necessary for that purpose.

However, this Article 6(1)(b) security permission applies only to 'providers of electronic communications networks and services', not the much wider range of services and organisations covered by the Article 5 prohibition. Articles 6(2) and 6(3) permit processing for the purposes of quality of service; billing, interconnection payments, addressing fraudulent or abusive use of services; and, with end-users' consent, the provision of services to those end-users, but these exemptions are even narrower, being restricted to 'providers of electronic communications services' alone.

Thus it appears that the only organisations permitted to process electronic communications data for the purposes of security are providers of electronic communications networks and services (by Art 6(1)(b)). Any other organisation whose logfiles are collected 'in connection with the provision and the use of electronic communications services' is banned from using them for security purposes, by Article 5.

As discussed above, the phrase 'in connection with the provision…' was interpreted

broadly by the Article 29 Working Party when it appeared in the earlier *ePrivacy Directive*: covering at least webmail and other providers performing anti-virus and anti-spam filtering. The new Regulation's more inclusive Article 2(1) – adding 'and the use' – must therefore be interpreted as applying this Article 5 ban even more widely. In particular there seems little doubt that operators of network-connected computers who examine their logfiles to detect and respond to incidents do 'process data in connection with … the use of electronic communications services', so a high risk that this Regulation will reverse the *Breyer* judgment that currently permits them to use their logs 'to ensure the continued functioning' of their systems.

Amendments to the Regulation proposed by the European Parliament and Council add new activities to the scope of the Regulation, and thereby condemn all the organisations performing them to the same trap where they are both required (by the GDPR) and prohibited (by the *ePrivacy Regulation*) to process data that is necessary for network and information security. Council amendments proposed between 5th December 2017 and 4th May 2018 would apply to, and thereby bring into scope, anyone installing security updates on end-user devices (for example employers when maintaining the security of staff equipment) (Dec 2017, Article 8(1)(e)); anyone processing communications data for scientific or research purposes (Dec 2017, Article 6(2)(e)), for "statistical counting" (May 2018, Article 6(2)(e)&(f)), or "audience measuring" (May 2018, Article 8(1)(d)); and operators of emergency services (Dec 2017, Article 8(a)(f)). Parliament amendments from 23rd October 2017 add social media providers (Amendment 11), email service providers (now explicitly listed in Amendment 13), and providers of personal assistance services such as search and text-to-speech converters (Amendment 20). With no narrowing of the scope of Article 5 being proposed, all these organisations must be covered by its ban. Nor is there any expansion of the security permission in Article 6(1) to assist them: both Council (Article 6(4)) and Parliament (Amendment 72 to Article 6(1)(b)) propose including third parties working on behalf of a network operator, but there is no mention of the much wider range of organisations involved in the other activities that the Regulation seeks to control.

Recital 14 of the Commission's draft makes the problem clear: the information that all these organisations are prohibited from processing includes 'any information concerning the content transmitted … information concerning an end-user … data to trace and identify the source and destination of a communication … date, time, duration and the type of communication'. This is vital information for preventing, detecting, investigating and resolving information security incidents in all networked computers (Cormack, 2016, p.262). Text such as the Parliament's amendment 72 – 'neither providers of electronic communications services, nor any other party, shall further process electronic communications data collected on the basis of this Regulation' – may be intended to protect network users from their service providers but actually exposes them to much greater risk from those who break into networked computers and can no longer lawfully be detected.

3. Resolving the Conflict

The text of the draft Regulation thus contains a mismatch between a general prohibition that applies to all organisations within the Regulation's scope and a security permission that only covers network operators. As more organisations are brought into scope, the

impact of this gap increases. Organisations, other than network operators, that process personal data in networked computers are simultaneously required by the GDPR to protect those systems and the personal data they contain, but prohibited from doing so by Article 5 of the draft *ePrivacy Regulation*.

This result is particularly unfortunate, as it is clear from their amendments that both Council and Parliament wish to encourage organisations to keep their systems and data secure against attack. By May 2018 the Council had added the detection of both attacks and security risks to Article 6(1)(b) as permitted purposes (though still only for network operators); the Parliament's Amendment 72 to that Article is concerned to 'to maintain or restore the availability, integrity, confidentiality and security' of networks.

The simplest way to resolve this problem would be to supplement Article 6(1)(b) with a security permission that is not limited to network operators. This would restore the position under the *ePrivacy Directive*, with network and information security being a permitted purpose for anyone processing electronic communications data: under *ePrivacy Regulation* Article 6 for all organisations covered by that Regulation and under the legitimate interests basis of GDPR Recital 49 for any others. A suitable text might read:

> Article 6(x): Electronic communications data may be processed if it is necessary to maintain or restore network and information security, for the duration necessary for that purpose.

Neither Parliament nor Council has yet proposed such an amendment.

Instead the European Parliament's amendment 15 proposes, in effect, to copy GDPR Recital 49 into Recital 16 of the *ePrivacy Regulation*, declaring that it 'should not prohibit the processing of electronic communications data … for the sole purposes of network and information security'. However, it is not clear that this statement in a Recital can override the contrary statement in Article 1(3) that '[t]he provisions of this Regulation particularise and complement Regulation (EU) 2016/679'. As the Presidency of the European Council explain in on page 3 of their 11th January discussion paper: 'particularise' means that 'whenever the ePR and GDPR norms deal with the same subject matter, the ePR applies'. The Presidency is explicit that Articles 5 and 6 'particularise[] the GDPR for electronic communications data that constitutes personal data', so on the common subject matter of processing communications data for the purpose of security the *ePrivacy Regulation*'s Article 5/6 ban would overrule the GDPR's Recital 49 permission. Furthermore, the Parliament's amendment only covers the types of organisations listed in GDPR Recital 49, not the other data controllers subsequently added by the Article 29 Working Party guidance on breach notification and by the draft *ePrivacy Regulation* itself. Even though these are certain to need to process electronic communications data to protect their systems and the data they contain, Article 5 appears to prohibit them from doing so.

In May 2018 the Council proposed a new security permission in Article 8(da) that would allow "information from end-users' terminal equipment" to be collected if "it is necessary to maintain or restore the security of information society services, prevent fraud or detect technical faults". It is unclear whether this is intended to resolve the security problem for information society services (though not for other organisations caught in the Article 5 trap), particularly as it appears to contradict the statement made by the Council in April that "processing by a[n] information society provider … for purposes such as ensuring network and information security … is not covered by this Regulation" (Recital 8).

In any case, much of the electronic communications data needed for security operations – notably IP addresses – is typically not "from end-users' terminal equipment", but originates in equipment operated by their Internet Access Provider, such as Network Address Translation devices (M^{3}AAWG, 2012, p.2). Thus, at best, this new provision still leaves a significant gap in website operators' ability to collect and process the information they need to keep their services secure.

The current state of the draft *ePrivacy Regulation* – as of July 2018 – will therefore affect the security activities of different organisations in different ways.

- Network operators continue to be permitted to perform necessary processing of electronic communications data, by Article 6(1)(b);

- Operators of websites and other information society services are permitted to process information from terminal equipment (e.g. URLs), by Article 8(da); depending on interpretation their processing of other electronic communications data (such as IP addresses) may either be banned by Article 5, or else permitted – subject to the GDPR – by the latest Recital 8 amendments;

- Other organisations (such as employers and software providers) that fall within the scope of the Regulation appear to be banned from processing electronic communications data by Article 5.

Even if individual organisations are able to process the information they need to secure their own services, the use of different provisions and definitions for network operators (Article 6(1)(b)) and information society service providers (Article 8(da)) will hinder the exchange of information between these groups that may be essential for detecting, investigating and remediating complex attacks (Cormack, 2016, p.269).

4. Conclusion

The Parliament and Council amendments to the Commission's text have converted a draft law that was clearly harmful for information security into one that is hard to interpret, self-contradictory, and still contains significant gaps. Nonetheless all parties agree on the Commission's statement in Recital 5 that the Regulation '[should] not lower the level of protection enjoyed by natural persons under Regulation (EU) 2016/679': the European Parliament's Amendment 4 to the same Recital declares that '[o]n the contrary, it aims to provide additional and complementary safeguards take into account the need for additional protection as regards the confidentiality of communications'; the Council Presidency confirms in January 2018 that 'the overall aim should be not to lower the level of protection of fundamental rights as set by the GDPR'.

Since at least 2006, legislators and regulators have been increasingly clear that protecting confidentiality and other fundamental rights requires the operators of all network-connected computers to use both proactive and reactive processes to ensure the security of those computers and any personal data they may have access to. Most recently, the Article 29 Working Party's Guidelines on Breach Notification state on page 12 that: 'it is the responsibility of controllers and processors to put in place suitable measures to be able to prevent, react and address a breach'. As the Working Party recognises, wherever personal

data are held in network-connected computers, those protective measures will involve the processing of electronic communications data: '[f]or example, for finding some irregularities in data processing the controller or processor may use certain technical measures such as data flow and log analysers, from which is possible to define events and alerts by correlating any log data'. GDPR Recital 49 establishes a regime under which this can be done safely, to the benefit of data controllers, processors and all the individuals whose data they process. Any interpretation of the draft *ePrivacy Regulation* that hinders or prohibits organisations from doing this would clearly 'lower the level of protection of fundamental rights' and must therefore be rejected as contrary to the purpose of the Regulation.

Bibliography

Legislation

European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) Brussels, 10.1.2017 COM(2017) 10 final 2017/0003 (COD)

European Parliament, Report on the Proposed Regulation on Privacy and Electronic Communications (23/10/2017) A8-0324/2017 http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&mode=XML&reference=A8-2017-0324&language=EN [accessed 9th March 2018]

European Council, Examination of the Presidency Text (Brussels, 5 December 2017) 15333/17

European Council, Examination of the Presidency Discussion Paper (Brussels, 11 January 2018) 5165/18

European Council, Examination of the Presidency Text (Brussels, 13 April 2018) 7820/18

European Council, Examination of the Presidency Text (Brussels, 4 May 2018) 8537/18

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

Commission Implementing Regulation pursuant Art 16(8) of NIS Directive C(2018)471 http://ec.europa.eu/info/law/better-regulation/initiatives/c-2018-471_en [accessed 5th July 2018]

Article 29 Working Party, Opinion 2/2006 on privacy issues related to the provision of email screening services (21 February 2006) 00451/06/EN WP 118

Article 29 Working Party, Guidelines on Personal data breach notification under Regulation 2016/679 (6 February 2018) 18/EN WP250rev.01

Cases

Patrick Breyer v Bundesrepublik Deutschland, ECJ Case C-582/14

Publications

Cormack (2016) Andrew Cormack, "Incident Response: Protecting Individual Rights Under the General Data Protection Regulation", (2016) 13:3 *SCRIPTed* 258 https://script-ed.org/?p=3180
DOI: 10.2966/scrip.130316.258

Forum of Incident Response and Security Teams (2018a) "FIRST History", https://first.org/about/history [accessed 5th July 2018]

Forum of Incident Response and Security Teams (2018b) "FIRST Teams", https://first.org/members/teams/ [accessed 5th July 2018]

M3AAWG (2012) "The implications of Large Scale NAT for Security Logging", https://www.m3aawg.org/sites/default/files/document/M3AAWG_Carrier_Grade_NAT_BP.pdf [accessed 5th July 2018]

---

[1] Chief Regulatory Advisor, Jisc Technologies