A review of Milaj (2015) and Rachovitsa (2016)

—

3,454 words

1 Introduction

In this article are discussed two articles on the subject of digital privacy.
In the first article,[1] Milaj details the proportionality principle that must be employed in determining whether or not a public authority is justified in breaching the rights to privacy of a subject in aid of maintaining a secure socity. She goes on to claim that a method is needed to allow police forces to assess the privacy impact of using technologies not intended for such activities as means of surveillance, in order to help them adhere to the proportionality principle and select the least invasive option at their disposal.
In the second article,[2] Rachovitsa discusses the concept of Privacy by Design as popularised following the Snowden leaks of mass global goverment surveillance, and provides evidence for the efficacy of furthering online privacy via technological means rather than statutory ones, followed by claims that legal and technological standards can cross-pollinate productively.
First, both articles shall be summarised and critiqued individually. Secondly, they shall be discussed together and compared.

2 Milaj (2015)

2.1 Summary

Milaj begins by summarising the notion of a 'right to privacy' provided by the European Convention of Human Rights,[3] and the various supportive bodies of case law. This right, however, is a '...non-absolute right...',[4] and Milaj describes the *proportionality principle* that is used to deter-

[1] Jonida Milaj, 'Privacy, surveillance, and the proportionality principle: the need for a method of assessing privacy implications of technologies used for surveillance' (2015) 30(3) IRLCT 115.
[2] Adamantia Rachovitsa, 'Engineering and lawyering privacy by design: understanding online privacy both as a technical and an international human rights issue' (2016) 24 IJL&IT 374.
[3] Convention for the Protection of Human Rights and Fundamental Freedoms (opened for signature 4 November 1950, entered into force 3 September 1953) 213 UNTS 221 (ECHR).
[4] Milaj (n 1) 115.

mine when the right may be infringed upon—the principle both '...protects fundamental rights and provides a justification for their limitation.' Moving through to the case law, she described the four questions to be used for determining proportionality, as laid out in the *Handyside*[5] judgement: '...that every "formality", "condition", "restriction" or "penalty" imposed [on a fundamental right] must be proportionate to the legitimate aim pursued.' Crucially for her later argument, she claims the decisions in *Marckx*[6] and *Gaskin*[7] as having established the requirement for the State to have '[. . . made] all the necessary positive arrangements to guarantee the effectiveness of the protection of the right.'[8] In short, the public authority that claims a need to infringe on the right to privacy must do everything in their power to limit that infringement. It is, however, '...clearly more desirable to prevent to cure'[9]—the means of determining whether the infringement is as minimal as possible must be *ex ante* rather than *ex post*.

Following this, Milaj reaches the crux of her argument—that '...national authorities require information that would enable them to authorize proportionate surveillance measures.'[10] With their obligation under the proportionality principle to display that they couldn not have '...adopt[ed] a less restrictive alternative',[11] they must have some means by which they can determine the privacy impact of subverting a particular device, not originally designed for such purposes, to surveil a target. This cannot, argues Milaj, be a statuatory means—a list, as it were, of '...those methods of surveillance and devices...explicitly provided in the laws.'[12] Rather, as '[. . . i]t is...quite impossible and improbable for legislation to keep the same speed as technology...',[13] the means must be information-based.

Milaj demonstrates this issue in the example situation of a police force that wish to find the location of an individual. '[M]ore than one device might be able to provide the same information'[14]—for example, the individual may carry on them a mobile phone for communicating with associates, a fitness tracker for tracking steps and a smart watch for *some* reason. Each of these devices, if compromised by the police force, would provide the GPS data needed to locate the owner. However, the additional data compromised—the 'noise' that comes along with the sought-after 'signal'—varies by device. The phone, for example, would also provide communications data, behavioural information and so on, whereas the fitness tracker would not. If the location data is all that the police force could reasonably be said to require, it is apparent that the mass collection of the ancillary data when a less-invasive means of acquiring the same required information exists would fail the test for proportionality—the state will have neglected their positive obligation towards the right to privacy.

[5] *Handyside v United Kingdom* (1976) 1 EHRR 737 .
[6] *Marckx v Belgium* (1979) 2 EHRR 330 .
[7] *Gaskin v United Kingdom* (1989) 12 EHRR 36 .
[8] Milaj (n 1) 118.
[9] ibid 118.
[10] ibid 120.
[11] ibid 119.
[12] ibid 120.
[13] ibid 120.
[14] ibid 120.

In order to determine the scope of privacy, Milaj lists the elements identified by Clarke,[15] Wright & Raab,[16] Borton et al[17] and Rojahn.[18] They are:

- privacy of the person;
- privacy of personal behavior;
- privacy of personal communications;
- privacy of personal data;
- privacy of location and space;
- privacy of thoughts and feelings, and;
- privacy of assocation.[19]

In addition to this, she introduces the 26 dimensions of surveillance identified by Marx,[20] ranging from audio to biometric information. Her theory is that, armed with information about which elements of privacy are infringed and which dimensions of surveillance are covered by compromising a specific device, national authorites will be able to choose the least-invasive option to still achieve their goals, according to the proportionality principle.
She goes on to detail a handful of current methods of potentially achieving this goal. The issue, she states, is that the existing measures '[...target...]technology designers and the private sector',[21] rather than law enforcement bodies. For example, much of the post-Lisbon Treaty[22] EU regulation is focused on data protection by commercial entitities, with limited focus on the issue of proportional privacy invasion by national authorities. 'It looks almost', she writes, 'as if the legislator wrongly believes that regulating data protection issues would itself solve the problems faced by the right to privacy.'[23]
For example, the idea of 'prior checking'—as found in the EU's Data Protection Directive[24]—requires that member states '...shall determine processing operations likely to present specific

[15]Roger Clarke, 'What's 'Privacy'?' (*rogerclarkecom*, 2006) ⟨http://rogerclarke.com/DV/Privacy.html⟩ accessed 20 January 2018.
[16]David Wright and Charles Raab, 'Privacy principles, risks and harms' (2014) 28(3) IRLCT 277.
[17]David Borton and others, 'An implantable wireless neural interface for recording cortical circuit dynamics in moving primates' (2013) 10(2) Journal of Neural Engineering.
[18]Susan Young Rojahn, 'A Wireless Brain-Computer Interface' (*MIT Technology Review*, 2013) ⟨https://www.technologyreview.com/s/512161/a-wireless-brain-computer-interface/⟩ accessed 20 January 2018.
[19]Milaj (n 1) 121.
[20]Gary Marx, 'What's New About the "New Surveillance"? Classifying for Change and Continuity' (2002) 1(1) Surveillance & Society 9.
[21]Milaj (n 1) 121.
[22]Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community (opened for signature 18 December 2007, entered into force 1 December 2009) [2007] OJ C306/01 (Lisbon Treaty).
[23]Milaj (n 1) 122.
[24]Directive 95/46/EC of the European Parliament and of the Council 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 [1995] OJ L281/31 (Directive 95/46/EC).

risks to the rights and freedoms of data subjects and shall check that these processing operations are examined before they start.'[25] However, the nature of an EU directive means that implementation varies across the EU members states. In many of these member states, law enforcement activites are not included within the scope of prior checking. Additionally, art. 33 of the upcoming GDPR[26] excludes from the scope of its proposed data protection impact assessment requirement '...the processing of personal data for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.'[27]

Other methods include the currently-used Privacy Impact Assessment (PIA) and the proposed Surveillance Impact Assessment (SIA).[28] PIAs are a device-focused approach that aims to promote the philosophy of 'Privacy by Design' by requiring an analysis of the privacy implications '...of a project, policy, programme, service, product, or other initiative...'[29] at an early stage. An SIA, in comparison, focuses on '...the subjects of surveillance, being individuals or entire groups of population.'[30] It assesses how new or planned-to-be-modified surveillance projects will impact society. Milaj takes issue with both assesments: the process of performing a PIA, she says, '...focus[es] almost entirely on data protection, not covering the other aspects of privacy...',[31] whilst the SIA is seemingly '...limited to projects designed for the purpose of surveillance...',[32] whereas the issue is the co-option of general-purpose devices for such purposes.

Finally, she presents Thommesen & Andersen's[33] proposed matrix for '...assessing the privacy "cost" of a surveillance system...',[34] based around (a subset of) the dimensions of privacy and surveillance previously discussed. Milaj praises the proposal for '...covering more aspects of privacy than the other methods discussed so far...',[35] but nonetheless takes umbrage with the fact that the matrix does not cover all the aspects of privacy thusfar identified, that it ignores the impact of a device on the privacy of third parties, and other shortcomings.

Prior to her conclusion, Milaj again summarises the faults of each current privacy assessment method. Finally, she wraps up with a final exhortation that '...the authorities need to have informaiton on the surveillance possibilities and on the intereference with the private lives of the individuals that will result from the surveillance measures and devices the authorities authorize to be used.'[36] She ends by stating that '...further research is needed.'[37]

[25] Milaj (n 1) 122.
[26] Regulation 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) [2016] OJ L119/1 (GDPR).
[27] Milaj (n 1) 122.
[28] David Wright, Michael Friedewals, and Raphaël Gellert, 'Developing and testing a surveillance impact assessment methodology' (2014) 5(1) Internatonal Data Privacy Law 40.
[29] Milaj (n 1) 123.
[30] ibid 124.
[31] ibid 123.
[32] ibid 124.
[33] Jacob Thommesen and Henning Boje Andersen, 'Privacy Implications of Surveillance Systems' [2009] Privacy Implications of Surveillance Systems.
[34] Milaj (n 1) 124.
[35] ibid 125.
[36] ibid 127.
[37] ibid 127.

2.2 Analysis

Milaj has successfully identified a genuine shortcoming in the tools available to law enforcement officials when it comes to ensuring proportional invasions of privacy in the interests of maintaining the rule of law. Her characterisation of the proportionality principle appears robust and supported across multiple bodies of European case law. She details a range of existing methods, along with their shortcomings. The article has, alas, numerous shortcomings of its own, the most egregious of which are the issues of scope, anticlimax and naïveté.

The first issue is that the article is uniquely focused on the issue of privacy within the European legal system. Despite having been published in the *International Review of Law, Computers & Technology*, there is no consideration of, for example, how the situation is presented within the US legal system. As the US right to privacy is not a codified right within the Bill of Rights, but part of the penumbra of derived rights,[38] this could have been an interesting avenue of further exploration. Indeed, does the concept of a proportionality principle even exist across the Atlantic? From a lay perspective, it appears that an echo of the European proportionality principle exists in the Eighth Amendment's prohibition of '...cruel and unusual punishments...', and in Justice Brennan's judgement in *Furman v Georgia* that described part of the test for such as looking for '[a] severe punishment that is patently unnecessary'.[39] However, Milaj has nothing to say on the subject.

The second issue is one of anticlimax. Having delineated the issue and listed the limitations of the current tools, Milaj fails to suggest any solution of her own. She details the various insufficient methods throughout §4, and then does so again through §5. This appears unnecessary, and it does not appear that any new insights are presented this second time through the same material. This wasted real estate of the article could certainly have been better utilised in the presentation of a solution to the identified problem. Instead, Milaj is content to pass the buck onto others with the concluding statement that '...further research is needed.'[40]

This dereliction of duty is particularly confusing, considering the nature of Milaj's criticisms of Thommasen & Andersen's matrix. She concedes that '[. . . t]he matrix created has the benefit of covering more aspects of privacy than the other methods discussed so far...', but complains that 'it does not cover them all.'[41] Her sole issue with the matrix, as presented in the article, is that it fails to take into account the additional dimensions of privacy and surveillance that have been proposed by others subsequent to its publishing. If these more recent additions to the canon of privacy are, as Milaj clearly considers them to be, of equal importance to those that were included in the original matrix, extending the matrix to include them strikes one as a trivial effort—not, however, one that Milaj makes.

Finally, there is the issue of potential naïveté. Milaj assumes that the national authorities will, when presented with multiple means of accomplishing the same goal—surveillance of a target in

[38] *Griswold v Connecticut* 381 US 479 (1965).
[39] *Furman v Georgia* 408 US 238 (1972).
[40] Milaj (n 1) 127.
[41] ibid 125.

one or more of Marx's dimensions—choose the most minimally-invasive option if only they are given the information needed to determine that. Milaj expressly states that she does not believe that such admirable self-control requires legislation to ensure it. This seems *optimistic*, to say the least. There are plentiful examples that demonstrate those same authorities' desire to push far beyond the bounds of proportionality when it comes to surveillance. These impulses have, repeatedly, been held in check only by the courts. The Data Retention and Investigatory Powers Act 2014[42] was struck down only by the decision of the ECJ in *R (Watson) v Secretary of State for the Home Department*;[43] it appears this decision had sounded the death knell of some of the more abhorrent elements of the subsequent Investigatory Powers Act 2016,[44] too. Across the Atlantic, *ACLU v Clapper*[45] and *Klayman v Obama*[46] demonstrated that this urge is universal to all national authorities; the recent reauthorisation of section 702 of the Foreign Intelligence Surveillance Act[47] of the also showed that not all legal systems are strong enough to resist it.

3 Rachovitsa (2016)

3.1 Summary

Rachovitsa begins by detailing the pervasive threat of '...mass and indiscriminate surveillance...'[48] in today's world. It undermines a vital prerequisite needed for the exercise of other human rights, undermines the rule of law and undermines trust in the digital economy. She then outlines the current approach of the Internet standards-setting bodies—that approach being one of 'Privacy by Design'.

After introducing the article, Rachovitsa briefly outlines the approaches to privacy of the Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB). The IETF, for example, view it not '...as a human right per se, or as a legal consideration, but rather as an instrumental value that must be understood as a necessary condition for restoring and maintaining users' trust in the Internet.'[49] She points out that '...Internet standard-setting does not observe formalities traditionally associated with the production of domestic or international law...'[50] and combines this with the observation that, '[a]lthough Internet standards are not legally binding, industry, organisations, Internet users and states adhere to and implement them.'[51]

This leads Rachovitsa to think that technical standards can serve as an unexpected means of ensuring change where legislation fails. 'Even though the perception of the technical solution as

[42] Data Retention and Investigatory Powers Act 2014 2014.
[43] Joined Cases C-203/15–C-698/15 *R (on the application of Watson) v Secretary of State for the Home Department* [2016] OJ /.
[44] Investigatory Powers Act 2016 2016.
[45] *American Civil Liberties Union v James Clapper* 785 F4d (2d Cir 2015) 787 (2015).
[46] *Klayman v Obama* 957 F Supp 2d 1 (DC DCC 2013).
[47] Foreign Intelligence Surveillance Act 1978.
[48] Rachovitsa (n 2) 376.
[49] ibid 376.
[50] ibid 378.
[51] ibid 378.

replacing or displacing the law could lead to a technocratic government of experts...',[52] Rachovitsa is unphased. 'The geeks will save the Internet and privacy',[53] she paraphrases. This is not, she argues, a call to politicise neutral standards-making bodies—the IETF's mission statement itself states that '[t]he Internet isn't value-neutral and neither is the IETF.'[54] The IETF and IAB interpret privacy through the lens of technical necessity rather than loftier human rights concerns. Without privacy, there can be no trust. Without trust, there can be no Internet.

There follows a *lengthy* overview of the technical concerns regarding Internet privacy. As the Internet was originally built and designed for use by '...a community of like-minded professionals who trusted each other',[55] privacy was originally left to the end-user in order to keep the protocol specifications as lightweight as possible. As part of the change of culture, the first 'privacy vocabulary' has recently been produced by the IAB.[56]

Rachovitsa goes on to describe the cultural differences between different cultural approaches to privacy. Whereas Western countries, through their inherited Enlightenment values, place strong emphasis on the rights of the individual, this is by no means a universal view. To consider it as such is dangerously Eurocentric and limits the hope of reaching agreement with the representatives of such other nations, argues Rachovitsa. Even in the West, views vary—the United States can appear rabidly individualistic in comparison to the social democracies of Western Europe. Having previously established that privacy online is not a matter of rights, but one of basic technical function, Rachovitsa claims that the solution to getting less indivudally-minded nations on board is through technical regulation. This avoids thorny moral quandries in favour of economics.

3.2 Analysis

There is, spread sparsely throughout the article, a point being made. Rachovitsa makes a strong case, supplemented with the IETF and IAB's own reasoning, for privacy being a vital prerequisite to the successful operation of the Internet on a purely technical level. If one was to write a paper stating that people would refuse to open bank accounts unless the amounts contained within were guaranteed to be private, they would be ridiculed for having bothered to announce something so obvious. That this same acknowledgement is not pervasive when it comes to the Internet is disappointing, to say the least.

Additionally, the use of built-in, technical means to ensure privacy is guaranteed to be more resistant to governmental abuse than a legislated means. Legislation is made by those same governments, and can be changed by them when their priorities change. Math is not, and can not. If the Internet protocols mandate that all traffic must be encrypted, and if these standards are implemented (and done so correctly) by vendors, then government's hands are tied when it comes

[52] Rachovitsa (n 2) 379.
[53] ibid 379.
[54] Harald Alvestrand, RFC 3935: A Mission Statement for the IETF (2004).
[55] Rachovitsa (n 2) 382.
[56] Alissa Cooper, RFC 6462: Report from the Internet Privacy Workshop (2012).

to traffic interception—the Internet is defined by its protocols, and if those protocols are built to be private, then there is little someone can do short of creating their own alternative network that lacks these provisions. Who would use such an obviously-inferior product is a mystery.

The point about using technical necessity rather than moralistic appeals to ephemeral (and non-universal) 'human rights' in order to market privacy to more authoritarian regimes is Rachovitsa's most interesting. Pragmatism, however, has a hidden cost. This is duly evidenced in the free software–open source split within software development. The free software movement came first, '...effectively defin[ing] the term "free software", deliberately giving it a confrontational weight'.[57] They argue that software composed of code that users are unable to examine and modify themselves—'nonfree software'—is both unsafe *and* unethical.[58] Three decades of abuses and mistakes, both by governments and by businesses, appear to lend weight to the former claim, and the recent Spectre and Meltdown vulnerabilities went unnoticed for over a decade in part due to the closed-shop nature of CPU design.[59] On the ethical front, they argue that restricting people's rights to access their own possessions would lead to things like planned obsolescence—would you buy a car that you weren't allowed to open the bonnet of?

The open source movement split off from the free software movement in the 90s. They continued to advocate for open code on practical concerns, but dropped the talk of ethics and of 'rights', such as the right to modify things one owns. The movement took off soon after, as businesses found the more pragmatic ideas easier to digest. Now, we live with almost everything that the free software activists warned of back in the 80s. Planned obsolescence in Apple phones,[60] technologies orphaned forever by restrictive licenses[61] and DRM now written into the very standards of the World Wide Web.[62]

The concern here is that the moral absenteeism of the open source movement parallels what Rachovitsa is proposing here, with the risk of its consequences following too. It is a good thing to be able to export privacy to these other countries, but what is it worth without exporting the *why?* behind it? This would certainly have been an interesting avenue of investigation within the article, but Rachovitsa loses interest almost as soon as she has begun—this is particularly frustrating in the light of the rest of the article, in which one must wade through swathes of verbiage in order to reach the small kernels of insight sprinkled throughout.

[57] Eric S Raymond, 'Homesteading the Noosphere' [1999] The Cathedral & the Bazaar.

[58] Richard Stallman, 'What is free software?' (*GNUorg*, 2001) ⟨https://www.gnu.org/philosophy/free-sw.html⟩ accessed 21 January 2018.

[59] Graz University of Technology, 'Meltdown and Spectre' (*spectreattackcom*, 2018) ⟨https://spectreattack.com/⟩ accessed 21 January 2018.

[60] BBC News, 'Apple investigated by France for 'planned obsolescence" (*BBC News*, 2018) ⟨http://www.bbc.com/news/world-europe-42615378⟩ accessed 21 January 2018.

[61] Anthony John Agnello, 'Nothing Lasts Forever: Confronting the Problem of Video Game Preservation' (*USgamer*, 2014) ⟨http://www.usgamer.net/articles/nothing-lasts-forever-confronting-the-problem-of-video-game-preservation⟩ accessed 21 January 2018.

[62] Cory Doctorow, 'Amid Unprecedented Controversy, W3C Greenlights DRM for the Web' (*EFForg*, 2017) ⟨https://www.eff.org/deeplinks/2017/07/amid-unprecedented-controversy-w3c-greenlights-drm-web⟩ accessed 21 January 2018.

4 Comparative Review

Milaj and Rachovitsa are both concerned with non-legislative means of ensuring privacy. Milaj believes that legislation moves too slowly to keep up with technology; Rachovitsa believes that legislation requires Western philosophies that may not be universal, and that the government that crafts that legislation will attempt to override it when it suits them. Both approaches are interesting, but both seemed flawed. Milaj believes that the national authorities will voluntarily choose to limit their invasions of privacy without having to be told to, despite all evidence to the contrary; Rachovitsa is willing to cede the moral territory in favour of pragmatism.

The two articles differ in a stylistic sense, too. Whilst Milaj's article would have been better served being longer, allowing her to prospose any sort of solution to her identified problem, Rachovitsa's is direly in need of an editor. She spends far too long describing the intricacies of the IETF and IAB and repeats herself throughout—the phrase 'Privacy by Design' appears 11 times alone on one page. Milaj is more concise, and thus far more readable, but even she repeats herself unnecessarily in §5.

From a perspective of rigour, however, both are rather more successful. The arguments put forward by both appear heavily supported by the corpus of European case law and both EU and national legislation, even though it would have been interesting to have seen a more international focus on Milaj's part.

5 Conclusion

Two articles of varying quality have been discussed, analysed and compared. Both examine means of ensuring privacy without resorting to legistation—one by identifying a current gap, the other by describing an existing phenomenon. One is more feasible than the other, but lacks an important moral dimension in favour of ruthless utilitarianism. Ultimately, however, legislation still appears necessary for reigning in some of the worse impulses of our governments, as evidenced by a string of recent (and not-so-recent) examples of case law from all over the world.

References

Agnello AJ, 'Nothing Lasts Forever: Confronting the Problem of Video Game Preservation' (*USgamer*, 2014) ⟨http://www.usgamer.net/articles/nothing-lasts-forever-confronting-the-problem-of-video-game-preservation⟩ accessed 21 January 2018.

Alvestrand H, RFC 3935: A Mission Statement for the IETF (2004).

American Civil Liberties Union v James Clapper 785 F4d (2d Cir 2015) 787 (2015).

BBC News, 'Apple investigated by France for 'planned obsolescence" (*BBC News*, 2018) ⟨http://www.bbc.com/news/world-europe-42615378⟩ accessed 21 January 2018.

Borton D and others, 'An implantable wireless neural interface for recording cortical circuit dynamics in moving primates' (2013) 10(2) Journal of Neural Engineering.

Clarke R, 'What's 'Privacy'?' (*rogerclarkecom*, 2006) ⟨http://rogerclarke.com/DV/Privacy.html⟩ accessed 20 January 2018.

Convention for the Protection of Human Rights and Fundamental Freedoms (opened for signature 4 November 1950, entered into force 3 September 1953) 213 UNTS 221.

Cooper A, RFC 6462: Report from the Internet Privacy Workshop (2012).

Data Retention and Investigatory Powers Act 2014 2014.

Klayman v Obama 957 F Supp 2d 1 (DC DCC 2013).

Directive 95/46/EC of the European Parliament and of the Council 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 [1995] OJ L281/31.

Doctorow C, 'Amid Unprecedented Controversy, W3C Greenlights DRM for the Web' (*EFForg*, 2017) ⟨https://www.eff.org/deeplinks/2017/07/amid-unprecedented-controversy-w3c-greenlights-drm-web⟩ accessed 21 January 2018.

Joined Cases C-203/15–C-698/15 *R (on the application of Watson) v Secretary of State for the Home Department* [2016] OJ /.

Handyside v United Kingdom (1976) 1 EHRR 737.

Marckx v Belgium (1979) 2 EHRR 330.

Gaskin v United Kingdom (1989) 12 EHRR 36.

Foreign Intelligence Surveillance Act 1978.

Furman v Georgia 408 US 238 (1972).

Graz University of Technology, 'Meltdown and Spectre' (*spectreattackcom*, 2018) ⟨https://spectreattack.com/⟩ accessed 21 January 2018.

Griswold v Connecticut 381 US 479 (1965).

Investigatory Powers Act 2016 2016.

Marx G, 'What's New About the "New Surveillance"? Classifying for Change and Continuity' (2002) 1(1) Surveillance & Society 9.

Milaj J, 'Privacy, surveillance, and the proportionality principle: the need for a method of assessing privacy implications of technologies used for surveillance' (2015) 30(3) IRLCT 115.

Rachovitsa A, 'Engineering and lawyering privacy by design: understanding online privacy both as a technical and an international human rights issue' (2016) 24 IJL&IT 374.

Raymond ES, 'Homesteading the Noosphere' [1999] The Cathedral & the Bazaar.

Regulation 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) [2016] OJ L119/1.

Rojahn SY, 'A Wireless Brain-Computer Interface' (*MIT Technology Review*, 2013) ⟨https://www.technologyreview.com/s/512161/a-wireless-brain-computer-interface/⟩ accessed 20 January 2018.

Stallman R, 'What is free software?' (*GNUorg*, 2001) ⟨https://www.gnu.org/philosophy/free-sw.html⟩ accessed 21 January 2018.

Thommesen J and Andersen HB, 'Privacy Implications of Surveillance Systems' [2009] Privacy Implications of Surveillance Systems.

Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community (opened for signature 18 December 2007, entered into force 1 December 2009) [2007] OJ C306/01.

Wright D, Friedewals M, and Gellert R, 'Developing and testing a surveillance impact assessment methodology' (2014) 5(1) Internatonal Data Privacy Law 40.

Wright D and Raab C, 'Privacy principles, risks and harms' (2014) 28(3) IRLCT 277.