UTRECHT JOURNAL OF
INTERNATIONAL AND EUROPEAN LAW

Aernout Nieuwenhuis, 'Review of *Privacy vs Security*' (2015) 31(80) Utrecht Journal of International and European Law 137, DOI: http://dx.doi.org/10.5334/ujiel.cy

BOOK REVIEW

Review of *Privacy vs Security*

Privacy vs Security, Sophie Stalla-Bourdillon, Joshua Philips and Mark D. Ryan, Springer, Springer Briefs in Cybersecurity, pp. 1–115, Softcover: €52.99, 2014, ISBN: 9781447165293

Aernout Nieuwenhuis[1]

[1] Associate Professor of Constitutional Law, University of Amsterdam, Affiliate member of the Institute for Information Law, the Netherlands

Keywords: security; privacy; data protection; data retention

Government measures to increase security more often than not lead to interferences with the right to privacy, for example the wide scale monitoring of telecommunication. Nobody will have missed the Snowden disclosures in this respect. These disclosures particularly concerned forms of surveillance outside the legal framework. However, government authorities are also authorised by law to process a large amount of personal data regarding their citizens' behaviour. Aside from government surveillance, in terms of corporate data collection, millions of Google users implicitly seem to accept that their searches are permanently registered by Google. They have no qualms with sharing all kinds of personal information on Facebook. Some writers therefore conclude that the era of privacy protection has come to an end, giving three kinds of arguments. First, a digital society wherein almost everything will be registered leaves less and less room for privacy interests. Second, many people are simply not interested in their informational privacy. Third, the interests involved in preventing terrorist attacks and discouraging organised crime are considered more important than privacy interests.

The authors of *Privacy vs Security* reject these views. The book starts by asserting that proponents of privacy protection are fighting more than a rear-guard battle. Nevertheless, the authors acknowledge that the right to privacy is under pressure and the near future may bring new challenges. They point, *inter alia*, to the increased sophistication of facial recognition techniques. It is not inconceivable that in the future a camera, or Google glasses, connected to a database would immediately supply all kinds of data concerning passers-by in, for instance, a shopping district or around a schoolyard.

Privacy vs Security is a somewhat incoherent book; it actually includes two relatively disjointed contributions. In the first part, comprising three quarters of the book, Sophie Stalla-Bourdillon starts by focusing on the European approach to privacy, as an interplay of privacy law, data protection and data retention law. Subsequently, she tries to clarify how to balance privacy and security and, more particularly, how to scrutinise the appropriateness of government measures in this respect (p. 2).

The right to privacy's characterisation in Europe is to a large degree based on the European Court of Human Rights (ECtHR) case law. The right to respect for private life, as laid down in Article 8 of the European Convention on Human Rights (ECHR), not only concerns protection against unlawful surveillance, but is more generally connected to an individual's personal development. In other words, it is not only a right to secrecy, but a right to liberty as well; the Court considers personal autonomy as an underlying principle. In short, Article 8 ECHR is meant to protect human dignity. Because of this setting, Article 8 ECHR deigns to offer a relatively strong protection against government interferences, including interferences concerning personal data. This perspective explains why the author is not that happy with the distinction made in the EU's European Charter on Fundamental Rights between the right to respect for private life (Art. 7) on the one hand and on the other hand the right to data protection (Art.8), that is sometimes allotted a lower position in the hierarchy of fundamental rights. One may doubt whether the distinction made in the European Charter is a real problem. One may point to the *Digital Rights Ireland* judgement of the Court of Justice of

the EU, welcomed by the author, that quashed the Data Retention Directive. The judgement is based on Articles 7 and 8 of the European Charter, without making a real distinction.

Another argument brought forward by the author may also be explained by the description of privacy in the light of the case law of the ECtHR. The 'good' citizen's reasoning 'no problem, nothing to hide' is of limited value. Privacy does not only regard discreditable information. First, almost everybody attaches importance to their intimate life's privacy. Almost no one would like to see their medical records lying in the street. Second, the interplay between privacy and security is not a zero sum game, for example protection against data phishing and identity theft protects both interests.

The author classifies the relevant ECtHR case law into four categories: 1. interception of telecommunication; 2. monitoring of telecommunication; 3. collection and storage of information relating to a person's physical identity; 4. collection and storage of information that is publicly accessible. In all these cases, the Court stresses in particular the requirement that an interference has to be 'according to the law', as required by Article 8 ECHR. That does not mean that an individual has to foresee that he is actually under surveillance, but that the regulation on which the interference is based has to provide for the necessary guarantees against abuse of power. The regulation must *inter alia* clarify in what circumstances what powers may be used by whom for what period of time. Moreover, there has to be a sufficient degree of control by other agencies. In some cases, defects in those respects have resulted in the conclusion that Article 8 ECHR had been violated.[1]

Nevertheless, the author characterises the Court's judgements, especially in national security cases, as deferential or too deferential. In *Weber and Saravia*,[2] for example, the Court implicitly seems to accept the possible use of extensive mass surveillance measures, including in other cases than those concerning the prevention of terrorism. In *Liberty*, the opinion that the regulation as such is to be considered acceptable, is followed by the conclusion that there has not been a violation, without any effort to look at the necessity of the possible interference in the circumstances of the case concerned. Yet the author is hopeful that the *Segerstedt* case[3] may be the beginning of a less deferential period; the Court concluded that even national security interests could not justify the keeping of the records with correct information about the participation in left wing demonstrations, which took place more than thirty years ago. One swallow in Strasbourg does not a summer make, however, because the Court generally follows a case-by-case approach.

In any case, national security's special position should not be interpreted extensively, according to the author. Public security, for example, has a much wider meaning. New concepts such as cybersecurity have to be scrutinised before being applied, because they often cover crime prevention in general or even economic welfare. For that matter, the author does not find certain measures appropriate as far as the prevention of terrorism is concerned. For example, measures based on profiling are hardly appropriate, because of the small number of terrorists attacks and the extensive interferences applied.

Positive obligations based on Article 8 ECHR oblige the government to lay down clear regulations as far as the processing of personal data by corporations is concerned. These rules must do justice to the privacy interests at stake. In this respect, the EU directives in this field do not satisfy the author; they are rather considered to be a guideline for data processors than a privacy document. Stalla-Bordillon's fear that data protection will be treated as a child of a lesser god than privacy is connected to this characterisation.

The author's argument supports her conclusion. On the one hand, governments should be less eager as far as collecting, registering and using personal data is concerned. The proportionality should be examined more strictly. On the other hand, governments should be more eager to protect privacy interests by regulating data processing by telecommunication companies and internet providers. To realise this, author's hopes are pinned down on a more robust interpretation of Article 8 ECHR by the ECtHR.

The courts play a less prominent part in the book's second part. The authors, Joshua Philips and Mark D. Ryan, stress the importance of the government's public accountability and democratic opinion forming. First they classify several kinds of privacy breaches by distinguishing on the one hand between big brother (the government), middle brother (corporations) and little brother (individuals), and on the other hand between lawful interferences (government access to registered data in accordance with the law) and more devious operations.

Their contribution focuses on government interferences and the lack of transparency thereof. To increase the public's awareness, they propose creating facilities for citizen's access to government's actions. In the

[1] F.e. Huvig v France, App no 11105/84 (ECHR 24 April 1984); Liberty v U.K., App no 58243/00 (ECHR 1 July 2008).
[2] Weber and Saravia v Germany, App no 54934/00 (ECHR 29 June 2006).
[3] Segerstedt-Wiberg v Sweden, App no 62332/00 (ECHR 6 June 2006).

first place, a dependable system has to be organised; every time the government looks into a database to collect personal data, the when, what and whom should be automatically marked in a log. The authors include a more technical description of how this can be made possible.

In his turn, a citizen should have access to certain data collected in these logs. One could consider the data regarding the government retrieving and storing information about him or herself, for example information from the public transport data base about his travelling pattern or information about mobile phone use. This may be compared to the so-called notification procedure, that plays a certain part in the system of checks and balances required by the ECtHR in case of surveillance measures; the subjects of surveillance should be notified afterwards. In practice, the part played is more dubious, because the notification may be postponed substantially or even renounced on security grounds. The authors propose a standard period of two years, without making clear however if this period starts immediately after the retrieval of the information, or after the security or police operation that triggered the retrieval has ended. In the latter case, the whole system becomes more complicated.

Especially interesting is the authors' idea that citizens should have permanent access to information, based on the logs mentioned, about the amount of data retrievals by the government, in a certain week, or in a certain town, and so on. This would provide for quantitative accountability as an important complement to the existing procedural checks and balances, being for the main part out of citizens' sight. Such a system would make governments more accountable to citizens (p. 111) who may decide for themselves if the interferences are overdone.

At first sight, that seems to be an interesting idea, apart from the question of whether the government might not get around such a 'watertight' system. The increasing government knowledge about citizens' actions will be countered by an increasing citizens' knowledge about the government's actions, by using more or less the same technical means. However, a number of problems may arise. It is, for example, not impossible that the transparency required can to a certain extent reveal the preparation of large scale police operations in a certain town, thereby threatening necessary law enforcement actions.

Nevertheless, I would say, the authors are not mistaken to emphasise quantitative accountability. For example, why do the annual reports of the Dutch Intelligence and Security Agency (AIVD) not give a summary of the amount of phone taps and other privacy breaches? Such information does not need to affect the agency's effectiveness, but gives the citizen some idea of security's privacy costs. Some form of quantitative accountability might even be an aspect of the checks and balances, required by the ECtHR when scrutinising surveillance regulations.

However, in neither part of the book can such an analysis be found. Therewith we touch upon the book's main flaw. The two contributions may be called chapters, the contributions' only coherence is the theme concerned, namely privacy vs security. Even the concept of privacy seems to differ. In this respect, the authors of the second chapter seem to have fewer objections against the automatic and encrypted registering of personal data than the first author.

The lack of coherence means that judicial review and quantitative accountability remain completely separate ideas. A very interesting question is, however, whether quantitative accountability may play a part in the more robust review of privacy breaches, desired by the first author. More generally speaking, only an interplay of judicial review, political accountability and other checks may restrain the government and protect privacy interests. In this respect, attention should also be given to the part played by the independent commissions supervising the intelligence agencies. The ECtHR also sees its role as an essential element of a system of checks and balances.

The book's lack of coherence does not make the book valueless, however. The first contribution provides for a treatment, worth reading, in particular of the approach of the ECtHR, as far as privacy breaches are concerned. The second contribution includes at least some interesting ideas on how to improve the government's accountability.

How to cite this article: Aernout Nieuwenhuis, 'Review of *Privacy vs Security*' (2015) 30(81) Utrecht Journal of International and European Law 137, DOI: http://dx.doi.org/10.5334/ujiel.cy

Published: 27 February 2015

]u[*Utrecht Journal of International and European Law* is a peer-reviewed open access journal published by Ubiquity Press.

OPEN ACCESS