Simon Chesterman, One Nation Under Surveillance – A New Social Contract to Defend Freedom Without Sacrificing Liberty

Oxford University Press 2011, ISBN 978-0-19-958037-8

by **Thomas Dreier,**
Dr. iur; M. C. J. (NYU); Director, Institute for Information and Economic Law, Karlsruhe Institute of Technology (KIT), Karlsruhe, Germany

Recommended citation: Thomas Dreier, Book review – Simon Chesterman, One Nation Under Surveillance – A New Social Contract to Defend Freedom Without Sacrificing Liberty, 2 (2011) JIPITEC 162, para. 1.

1 What do Saddam Hussein, information law, and privacy have in common? Not much, at first sight. However, a second glance reveals that they constitute key elements of what might be termed *public information law,* i.e., the body of legal rules that govern the relationship between public authorities – both governing and administrative – toward the citizens. This characteristic distinguishes it from private information law, which structures the informational relationships amongst private firms and individuals. It hardly comes as a surprise that the issue of regulating the obtaining and use of intelligence information has received particular attention in the US in the wake of the 2001 attacks and the subsequent "war on terror" launched immediately following by the Bush administration. Of course, these issues are discussed in Europe as well with regard to anti-terror legislation, today mostly regarding the question of its prolongation. In Europe in general, however, public information law is mostly discussed under the headings of informational self-determination, freedom of information acts, and public sector information (PSI). This places the focus on the administrative aspect and the public/private interface rather than on the legal regime governing the collection and use of intelligence information by state authorities, most notably their secret services, and, for some time, also by private contractors to which the collecting of intelligence information has been outsourced.

2 Compared with other types of information, intelligence information possesses some particular features, even if the boundary between intelligence and non-intelligence information may be difficult, if not impossible, to draw. Ultimately, any sort of information that is not generally available can be considered intelligence information. The important qualifier seems to be that the information in question is collected and used by an intelligence-collecting body as part of intelligence. The most prominent feature of intelligent information is that once it has been collected it is purposely kept secret. Even more, in order to keep the information secret once it has been collected, the process of collecting must itself be kept secret. From there, it is only a small – and for governments a rather tempting – step to keep even the existence of the intelligence-gathering body secret. Although the need for, and legitimacy of, both intelligence-gathering organizations and the secrecy they deploy is generally accepted as such, for democratic societies, which are based on the principles of control and, to a large extent, on transparency, it is particularly troublesome to draw proper lines regarding when secrecy is justified and when it should be lifted. The problem, of course, is how to learn about secret information in the first place. Moreover, even if a process for reviewing the real or perceived legitimacy of the secrecy is provided for, the question is which institution – internal or external, political or judicial – appears to be best suited to make the appropriate decisions. Finally, contrary to private information law, where conflicts between keepers and seekers of information as regards intelligence information can be decided by an independent third party – in general, the legislature, and in particular, the ju-

diciary – the executive and more often than not the legislature are themselves immediately involved as interested parties, making the role of the judiciary even more troublesome.

3 With his book, Simon Chesterman – Vice Dean and Professor of Law at the National University of Singapore, and Global Professor and Director of the New York University School of Law Singapore Program – who has extensively published on issues of international law, in particular on intelligence and security as well as on legitimacy and the limits of legality of state actions in this respect, obviously pursues two objectives. First, he gives a concise and comprehensive overview of the current legislation on gathering and using intelligence information as illustrated by the cases of the US and Britain in response to the real or perceived threats of globalized terror, but also by the different activities of the United Nations. Second, he discusses the different governance options to come up with a recommendation for how an appropriate framework for preventing abuses should be construed.

4 Consequently, the book is divided in three parts. Part one lays the theoretical foundations, beginning with an overview of the legal regulation of spies in times of peace and war, of consular activities under the guise of which – often tacitly accepted by the host country – intelligence gathering takes place, and of intelligence as such. This is followed by an account and discussion of the problem of emergency powers, both as regards their exercise in practice and their legal justification, which in spite of attempts to argue in a legal way, tends to limit, or at least demonstrates the limits of, the rule of law. At the end of the first part the author focuses on the need for state secrets, barriers to effective accountability, and extra-legal measures of intelligence gathering. Part two of the book then begins with the US up to the Bush administration change toward outsourcing state intelligence-gathering tasks to private contractors. With the United Kingdom, which the author has chosen as his second example, it becomes clear that in spite of the similarities of taking on the perceived threat of global terror, there was at least an attempt to maintain the rule of law, which is probably due to a different historical legal culture. This, however, accounts for the British indifference toward comprehensive CCTV surveillance as well as for the sensitivity of the British vis-à-vis the introduction of an identity card. As a third example, Chesterman has chosen not another individual state, but rather the United Nations. Here, the description of the numerous activities of the UN, its sub-organizations, and the special tribunals – none of which have intelligence information of their own but must rely on the making available of intelligence information by national secret services – reveals a much richer and more nuanced picture. This enables the author in part three of the book to examine the most appropriate structures available to ensure the accountability of intelligence services, and to consider whether the focus of accountability should be on the collection of intelligence or on its use. He then returns to the theme of whether and how intelligence activities can be regulated effectively in view of the diminishing sphere of truly private activity and the growing coercive powers of the state in the final chapter.

5 It is not the purpose of this review to focus on the issues of the regulation of intelligence activities in times of war and in peace in general, since this does not lie within the scope of a journal on IP- and IT-law. In addition, other commentators are much more qualified in this respect; it should only be noted here that although the book contains a general reference to whistleblowers, the reader will search in vain for a more detailed discussion of the usefulness and legitimacy of organizations such as Wikileaks. Depending upon which side you are on, you will either see in the book an account of "the privacy implications of the war on terror" (Frederick P. Hitz, former Inspector General, CIA) or you will conclude – more in line with Chesterman – that "often foreign and domestic intelligence gathering in the major democracies has been insensitive to public accountability, legality, and its consequences for individuals, to the detriment of both liberty and security" and "how ... this can and must change" (Gareth Evans, President Emeritus of the International Crisis Group and former Foreign Minister of Australia).

6 However, what is of importance for both the future of privacy and data protection is Chesterman's core thesis and, as a matter of fact, the fundamental assumption on which all other conclusions are based: In view of the ever-increasing data available to governments as well as the ever-increasing computing power that enables governments to combine, analyze, and profile the vast amount of data collected and stored, according to Chesterman it would be illusionary to try to re-establish privacy to a pre-computer age and to implement the principle of collecting as little data as possible. Rather, in his view, attention should more realistically be focused on the legitimacy of the *uses* made of such data. Refuting "false" or at least "misleading" choices, in particular the classical tradeoff between liberty and security ("how much freedom shall be sacrificed for how much security?"), and after having reviewed the different options available, Chesterman finally asks for a "new social contract" that should be characterized by three principles: (1) the intelligence powers exercised must be public, (2) the entities carrying out these functions must be legal, and (3) accountability for activities of intelligence services must be consequence-sensitive (as opposed to having the aim of deterring or responding to abuse). As Chesterman concludes himself: "These principles ... may sound obvious, if not trite. Nevertheless, as this book has shown, established democracies founded on the rule

of law and the most important international organizations ... have not lived up to them."

7 True, as such the book's primary focus is not on information law per se. Rather, its main impetus is to take an active part in shaping appropriate governance structures as regards the handling of intelligence information, and, ultimately, to preserve the rule of law which – between 9/11and the election of President Obama – has probably come more under attack in the US than in any other Western democracy. Obviously traumatized by the US experience of having suffered under the Bush administration which in many instances placed itself above the law, Chesterman analyzes the dangers that come with an unfettered collection and use of intelligence information. Although this is set against a US background, it should be noted that the title of the book ("*One* Nation under Surveillance") does not refer to the US alone; instead, it suggests not only that the issue is global, but likewise that only one solution is appropriate. But even if it is true that information gathering by intelligence services is no longer confined to national borders, making the classical distinction between internal and external information gathering blurred if not almost meaningless (though even this may be questioned in view of the fact that the US *demanded* European flight and credit transaction data from the EU), and if in this sense all the peoples of the world do indeed form "one" nation under surveillance, it is also true that the different cultures of the world should be taken together to form an appropriate response to the issues raised. Contrary to Chesterman, I would therefore argue that the attempt to exercise at least some fundamental sort of control over the collection of intelligence information should not be given up too easily. As a matter of fact, to cite just one national example, in 2010 the German Constitutional Court declared unconstitutional a law that obliged telecommunication companies to store all communications data, thus triggering a debate as to whether – and if so, under what circumstances – such a general storage should be permitted, and under which conditions state authorities may have access to, and make use of, the data thus collected. Also, different EU Member States have different opinions on this point. In sum, it appears that the key to the solution lies in a combination of *both* the control of *gathering and use* of intelligence information.