Book review: Valsamis Mitsilegas and Niovi Vavoula (Eds.), Surveillance and Privacy in the Digital Age: European Transatlantic and Global Perspectives. Oxford: Hart Publishing, 2021. 315 pages. ISBN: 9781509925179

Cite as follows: J.J. Oerlemans, 'Book review: Surveillance and Privacy in the Digital Age: European Transatlantic and Global Perspectives, edited by Valsamis Mitsilegas and Niovi Vavoula. (Oxford: Hart Publishing, 2021)', *Common Market Law Review*. Volume 59, Issue 3 (2022) pp. 951 – 952.

Reviewed by Jan-Jaap Oerlemans
Prof. dr. J.J. Oerlemans is an endowed professor of Intelligence and Law at Utrecht University

The aim of the book 'Surveillance and Privacy in the Digital Age: European Transatlantic and Global Perspectives' is ambitious. The editors seek to 'critically analyse the evolution and proliferation of surveillance paradigms in the digital age and their impact on fundamental rights'. To achieve this aim, 13 authors wrote a total of 10 chapters, divided in the following themes: 'The Challenge of Digital Evidence' (Part I), 'New Surveillance Challenges' (Part II) and 'Human Rights Responses' (Part III).

The focus of the book is on European criminal law and privacy law, as well as case law of the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU). In Chapter 7, it takes a welcome side step to a discussion of 'China's Surveillance State' and in Chapter 8 to 'UN Human Rights Instruments' addressing state surveillance. This focus of the book can be explained, because the majority of the chapters of the book were presented at the Annual Conference of the European Criminal Law Academic Network (ECLAN) on 'Privacy and Surveillance in the Digital Era', on 17-18 May 2018 in London.

Part I (Chapters 1-4) about 'The Challenge of Digital Evidence' really only focuses on a single challenge, namely the challenge of 'governmental access to data stored at electronic communication providers' in criminal investigations. The authors analyse the origin and evolution of legal frameworks that regulate access to stored data by law enforcement authorities. The chapters provide a good description of the E-Evidence initiatives of the European Commission and the U.S. CLOUD Act. The authors also identify the human rights issues involved with these instruments. At the time of the conference (in 2018), these were 'hot topics'. By 2022, many of these instruments have developed further. The papers submitted in the original conference seem to be updated until the end of 2020, but sometimes only marginally. For example, it misses an analysis of the first the bilateral agreement between the United States and the United Kingdom on 'Access to Electronic Data for the Purpose of Countering Serious Crime' in July 2020. Readers of the book should be aware that the legislation progressed in the meantime, such as the – only briefly mentioned - Second Additional Protocol to the Council of Europe "Budapest" Convention on Cybercrime (adopted in November 2021). Academics should analyse themselves whether the identified human rights issues that were identified at the time of writing, still remain.

Part II (Chapters 5-7) about 'New Surveillance Challenges' starts strong with a well-written overview about 'The Privatisation of Surveillance in the Digital Age' by Mitsilegas himself,

one of the editors of the book. Mitsilegas guides it readers through CJEU case law regarding data retention, from *Digital Rights Ireland* (2004) to *Tele2* (2016), but unfortunately not *La Quadrature* and *Privacy International* (2020). He then provides a critical analysis of both *Schrems*-cases regarding data transfers between the EU and US. The describes the more recent attempts of the European Commission to prevent the dissemination of terrorist content online and even discusses the 'model of privatised surveillance' in the context of responses to the management of COVID-19. The second editor, Vavoula, wrote an entirely different, but also strong, chapter about the 'Interoperability of EU Information Systems in a 'Panopticon' Union'. Her chapter is more focused on the specific problem of the proposed interoperability of EU information systems, which intensifies surveillance of 'mobile third-country nationals'. She takes in a strong position and characterises the development of interoperability as *"the latest nail on the coffin of third-country nationals' privacy"*. EU criminal law scholars could ask themselves: did these plans of interoperability and effects on fundamental rights materialised in the meantime? It may inspire new academics, such as PhD students, to pick up the topic and research it further.

Part III (Chapters 8-10) about 'Human Rights Responses', is significantly shorter than the other two parts of the book. However, it still provides a valuable overview of UN Human Rights instruments, EU law and ECtHR's case law in relation to surveillance. All three chapters are clearly structured and provide a nice overview. Chapter 10 about 'One European Legal Framework for Surveillance' from De Hert & Malgieri provides a more in-depth overview of ECtHR-case law relating to state surveillance. In six tables, the authors clearly identify important considerations and help readers navigate the ECtHR's case law.

To sum up, the book is good resource for EU criminal law scholars with a focus on privacy and data protection law. Readers should keep in mind most the chapters were originally based on papers written for a conference in 2018. The book could perhaps have been published two years earlier in 2019, but it still provides a good background and origin story of EU case law and legislation regarding digital surveillance. It may entice researchers, such as PhD candidates, to delve into specific topics addressed in the book and further contribute to the 'evolution of surveillance paradigms in the digital age and their impact on fundamental rights'. Just like the editors intended for the book.

Jan-Jaap Oerlemans
Utrecht