

BOOK REVIEW

State Sponsored Cyber Surveillance: The Right to Privacy of Communications and International Law by ELIZA WATT [Edward Elgar Publishing, Cheltenham/Northampton, MA, 2021, ISBN: 978-1-789-90009-5, 384pp, £120.00 (h/bk)]

In February 2024 the European Court of Human Rights (ECtHR) decided the first case examining the permissibility of a statutory requirement compelling internet service providers to support law enforcement efforts in decrypting end-to-end encrypted communications. *Podchasov v Russia* represents a milestone decision for the ECtHR. A unanimous bench found that policies weakening encryption and the security of communications, including through mandatory backdoors and compelled forms of assistance, are inherently disproportionate and violate the right to privacy. The decision sent a strong message about the vital importance of encryption for an ever-digitizing information society.

The case also demonstrated how the ECtHR continues to rely on its analytical framework for privacy protection, even when addressing new technological challenges. In its analysis, the ECtHR drew heavy guidance from its prior jurisprudence in cases such as *Roman Zakharov, S and Marper* and *Big Brother Watch*. Building on this case law, the ECtHR determined both the existence of an interference with the right to privacy and ruled out any justifications for that interference. Anyone who has read *State Sponsored Cyber Surveillance: The Right to Privacy of Communications and International Law* by Eliza Watt would be familiar with these cases and this framework. In this book Watt provides a rich account of the current frameworks governing the right to privacy in international human rights law (IHRL). The book thus offers an enduring frame of continued relevance, even in the face of new technological challenges.

Applying a doctrinal lens, Watt intricately dissects the paradox of securing national interests while safeguarding fundamental human rights, presenting her arguments over eight meticulously structured chapters. One of the book's core contributions is Watt's ability to bring together seamlessly two separate discourses in international law that rarely meet. The first is the discourse on cyber and internet governance and the second is the human rights discourse on digital rights protection. The central chapters of the book are devoted to the human rights analysis, addressing such issues as: the customary and treaty scope of the right to privacy (Chapter 3); the extraterritorial application of the right and its relationship with the principle of non-discrimination (Chapter 4); and the scope of the protection the right offers against unjustifiable interferences by agencies of the State (Chapters 5–6).

However, those human rights chapters are nestled between two sections of the book that ask even broader questions about international governance of


State surveillance activity. Watt does an excellent job distinguishing cyber surveillance from a wider universe of governmental espionage and election interference operations to highlight the way other domains of international law—from sovereignty to non-intervention—might supplement human rights law in regulating the intelligence function of the State (Chapter 2).

In her two concluding chapters, Watt gives careful attention to the prospect of a *lex specialis* that could emerge ‘at the international level to regulate the operational methods of intelligence and law enforcement agencies’ (328). Seeking to identify this elusive and emerging *lex specialis*, Watt explores a wide range of binding and non-binding instruments. In what is the book’s most ambitious effort, Watt examines domestic legislation (from the United States, United Kingdom, Russia and China), bilateral agreements, United Nations (UN) processes and a range of soft law international frameworks to locate potential *lex specialis* contenders (Chapter 7). She concludes that while a ‘cyber surveillance *lex specialis*’ is desperately needed, all proposals for such regulation have thus far been ‘met with a frosty reception’ (341). It is for this reason that she embraces the sober finding that ‘mass surveillance of digital communications is a reality’ (343). This finding entails that the legal battles of tomorrow—around the use of Internet of Things, artificial intelligence, Big Data Analytics and post quantum cryptography—will be fought with mass surveillance’s permissibility as a foregone conclusion, thereby condemning the possible scope and reach of these debates to an inescapable fate (Chapter 8). Consider the case of facial recognition technology (FRT) in criminal enforcement as an example. Watt’s core arguments seem to describe well the ECtHR’s recent response to the technology. In *Glukhin v Russia*, the Court chose to build on its existing framework, which by default assumes the necessity of bulk collection and analysis of data in criminal investigations. Far from developing a tailored or specialized regime to address FRTs, the Court implicitly affirmed the use of FRT by governments. Citing its existing case law, the Court thus declined to engage with civil society’s narrative that FRTs are categorically incompatible with IHRL.

In light of these findings, Watt’s central thesis is that a multilateral cyber surveillance treaty is necessary to rekindle and reorient this dialogue, ensuring that mass cyber surveillance does not become an irreversible norm. She briefly examines the short-lived effort in 2018 of the inaugural Special Rapporteur on the Right to Privacy, Professor Joseph Cannataci, to design a similarly minded Legal Instrument on Government-Led Surveillance and Privacy, as evidence that a treaty could materialize. Yet, Watt’s near-exclusive focus on formal treaty making and other institutional efforts at norm creation, predominately at the UN-level, is also one of the core limitations of her work. She writes: ‘an analysis of whether peacetime espionage can be said to form a rule of customary international law is beyond the scope of this book’ (85). This is where Watt misses an opportunity to think

more creatively about the emerging *lex specialis* of intelligence in international law. If she had shifted her attention to other sources—evolving customary practices, general principles of law—or even dared to think outside the box of positivism altogether, she might have been able to find other more subtle but also more tailored normative guidelines for the regulation of intelligence work. This is precisely what other scholars have done in examining the normative constraints on interstate intelligence, including Ashley Deeks (from within international law), Cécile Fabre (from within moral philosophy) and David Omand and Mark Phythian (from within intelligence studies), to name but a few. The various ethical and legal guidelines proposed by these thinkers could help fill gaps in the interim period, until political appetite for formal codification is found.

Despite this limitation, by intertwining theoretical frameworks with practical case studies, Watt deftly addresses the complexity of regulating State-sponsored surveillance activities. She sheds new light on a timely and entrenched problem and advocates for a balanced approach that does not compromise the core values of privacy and internet freedoms. The book is primarily aimed at human rights practitioners, cybersecurity policymakers, surveillance scholars, and students of international law and national security law. The book canvasses existing rules and policy solutions for cyberspace's most vexing challenges at a time when the need for such a resource has never been higher. As the world seems to enter a dangerous artificial intelligence arms race, Watt's book provides an invaluable map to support the continued advocacy efforts of digital rights defenders worldwide.

ASAF LUBIN 
Indiana University Maurer School of Law, Bloomington, USA
Email: lubina@iu.edu