International Journal of Legal Information 52.1, 2024, pp. 110–114.

BOOK REVIEWS

State Sponsored Cyber Surveillance: The Right to Privacy of Communications and International Law. Eliza Watt. Cheltenham, UK; Northampton, MA: Edward Elgar, 2021. Pp. 364. ISBN 978-1-78990-009-5. US$150.00.

There have always been spies. For as long as there have been secrets, there have been people (and governments) willing to use every technology at their disposal to discover them. However, while surveillance by nation-State actors is a decidedly ancient practice, the scope and scale of modern espionage now reaches far beyond what past spymasters could possibly have imagined. The cascading internet-facilitated connections of 21st-century life have created an unprecedented number of avenues for both passive and active surveillance, with intelligence services more than happy to take advantage. As this new covert paradigm burgeons in the shadows of the World Wide Web, it is far from clear how any of this technological voyeurism squares with the international legal order, including our most deeply cherished human rights. Who gets to leverage the awesome power of cyber surveillance, against whom, and for what purpose? British legal expert Eliza Watt fastidiously addresses these questions in her thoughtful and deeply researched text, *State Sponsored Cyber Surveillance: The Right to Privacy of Communications and International Law*. By exploring how different kinds of large-scale technological intrusions into private life fit within the current landscape of international law, Watt has created a compelling baseline for any future discussion of protecting online privacy.

The book's early chapters offer one of its greatest contributions—a comprehensive definitional exercise sketching the contours of several varieties of cyber spycraft. Moving beyond blunt and antiquated categories like Human Intelligence (HUMINT) and Signals Intelligence (SIGINT), Watt instead distinguishes three broad classes of internet-enabled intelligence operations: (1) Cyber Espionage, (2) Cyber Surveillance, and (3) Cyber Electoral Interference. In this conception, Cyber Espionage includes the non-consensual remote accessing, copying, collection, and/or storage of confidential information for either political ends or economic advantage (such as the theft of trade secrets). By contrast, Watt characterizes Cyber Surveillance as a national security practice aimed at the indiscriminate collection of communications information, consisting of either the mass interception of communications' contents or the bulk collection and retention of detailed data about communications (e.g., metadata). Cyber Electoral Interference is a more nuanced category, encompassing both computer-assisted tampering with election infrastructure and information operations that propagate misinformation or disinformation. It should be noted that this summary massively oversimplifies the carefully crafted multipart definitions Watt assembles. However, even these broad-stroke versions demonstrate the value these building blocks provide to scholars and policymakers, who can now use a controlled vocabulary when grappling with these often ill-defined issues.

Having established how the differences in these activities necessitate tailored international legal regimes, Watt then ably delves into the even thornier task of explaining how the amorphous concept of privacy is conceptualized and operationalized within existing international instruments and adjudicatory structures. This begins with a thorough inquiry into whether the right to online privacy has achieved the status of customary international law as defined in article 38(1)(b) of the Statute of the International Court of Justice. Despite broad, abstract consensus that human rights (including privacy) apply to the online environment, Watt determines that online privacy is at best an emergent rule and thus devotes the bulk of the remaining chapters to examining privacy's place within the existing human rights treaty landscape. While the material that follows is unquestionably the densest portion of the entire text, it is also the most insightful.

Watt first reviews how equality of treatment and nondiscrimination form the core of international human rights law, beginning with the 1946 Universal Declaration of Human Rights and reinforced by the UN International Covenant on Civil and Political Rights (ICCPR) and the European Convention on Human Rights (ECHR). She then examines whether having different rules for cyber surveillance of domestic versus foreign

https://doi.org/10.1017/jli.2024.16

individuals (as many nations do) constitutes a violation of these treaty principles and whether the duty to protect the right of privacy enshrined in the ICCPR, the ECHR, and the American Convention on Human Rights (ACHR) applies to the signatories' extraterritorial cyber-surveillance efforts. Building on this groundwork, Watt distills the privacy formulations of article 17 of the ICCPR, article 8 of the ECHR, and article 11 of the ACHR into a two-part test. The international organizations and tribunals tasked with enforcing these treaties must generally determine whether (1) there has been an interference with the right to privacy of communication, and if so, (2) whether that interference was justified. This is followed by a full two chapters methodically applying these legal standards to cyber surveillance, before contextualizing that analysis within a discussion of past (and potential future) efforts to directly address cyber security through multilateral instruments. As with Watt's definitional work, the preceding is a highly abbreviated overview of an extensive investigation; this format cannot do justice to the incredible depth of the analysis.

The text does have some shortcomings, often the result of necessary compromises in a book of this kind. While it is eminently readable for those versed in the field, it is not especially accessible otherwise. The prose is sprinkled with jargon and Latin legal phrases (such as *sensue lato*, *locus standi*, and *lex specialis*) that could alienate a broader audience. The level of detail, particularly in the later chapters, results in some sections that read as overwrought. These passages feel weighed down by excursions into minutia and slowed by an overreliance on block quotes that rarely add value commensurate with their lengths. Most notably, the work as a whole displays a strong focus on European tribunals and US/UK law. This is certainly understandable given the importance of this jurisprudence and the prominence of the US and UK in the cyber arena. However, it is the kind of restriction in scope that is worth mentioning for an academic reference text addressing an international topic.

That said, the work is still a remarkable achievement. Watt's *State Sponsored Cyber Surveillance* would be an excellent addition to any academic library but would be particularly at home in academic law libraries, government agencies, and on the desks of all policymakers or jurists who regularly confront transnational human rights issues.

Daniel Radthorne
Research Librarian, Arthur J. Morris Law Library
University of Virginia School of Law, Charlottesville, Virginia
doi:10.1017/jli.2024.16

Climate Change, Sustainable Development and Cleantech: A Pathway for Developing Countries. Joy Y. Xiang. Cheltenham, UK; Northampton, MA: Edward Elgar, 2022. Pp. 210. ISBN 978-1-78536-345-0. US$120.00.

Combating climate change will require a global effort, but the tools and resources for this fight are currently held by just a few affluent countries. How can we distribute these often-proprietary technologies to developing nations whose participation is vital to achieving international climate goals? Further, how can we do so while also incentivizing wealthy States to continue groundbreaking research and development in this field? These are thorny questions, but author Joy Y. Xiang is equal to the task in her meticulously constructed text, *Climate Change, Sustainable Development and Cleantech: A Pathway for Developing Countries*. With clear-headed analysis and precise prose, Xiang unpacks how intellectual property law and sustainable development can be cornerstones for the widespread adoption of new technologies designed to mitigate or adapt to climate change (so-called "cleantech").

Xiang begins with an efficient introductory chapter, sketching the contours of the underlying problem: intellectual property rights (or IPR) have been a long-running sticking point in the global climate response. Through multiple conferences and rounds of negotiations organized under the auspices of the UN Framework Convention on Climate Change (UNFCCC) and the World Trade Organization (WTO), developing countries have repeatedly pushed for a reduction in IPR protections for new cleantech. The thrust of these arguments is typified by a notable proposal presented by Ecuador at a 2013 WTO meeting. The proposal asserted that existing IPR regimes inherently facilitate the monopolistic hoarding of clean technologies by richer nations. To ensure knowledge transfer to the developing world, Ecuador suggested that cleantech should be categorically excluded from patentability or subject to compulsory licensing rules that require the technology to be shared at a fair price. While several developing countries supported the proposal (including major economies such as India, Brazil, and China), developed nations such as the United States balked. Instead, the latter suggested that instituting *stronger* IPR protections