Axel Arnbak, *Securing Private Communications. Protecting Private Communications Security in EU Law – Fundamental Rights, Functional Value Chains and Market Incentives*. Alphen aan den Rijn: Kluwer, 2016. 296 pages. ISBN: 9789041167378. EUR 133.

Arnbak's book has been published at a time when communication technology is as fascinating as it is troubling. The gestation of Arnbak's PhD thesis coincided with Edward Snowden unearthing unprecedented mass surveillance programmes. That revelation propelled the debate about data control and private communications to the fore of the public's consciousness. However, public opinion shifted rapidly when the European mainland was targeted in a series of terrorist attacks. Just recently, Donald Trump abolished the US-EU "Privacy Shield" – US privacy rights will only apply to US citizens. In addressing private communication, as elsewhere, the EU lawmaker thus finds itself facing radical new challenges.

This clear and well-structured book is largely based on Arnbak's PhD thesis, which was finished in the summer of 2015. Arnbak is a lawyer. Accordingly, he tries to resolve what is in essence a legal question. But in his pursuit of a solution, he is not afraid to borrow from other fields, most notably security economics and functional value chain analysis. The author scrutinizes legislative history and proposes regulatory solutions that might well shape the future of communication security.

The main research question, "how should the EU lawmaker protect private communications security?", guides the reader throughout. The book has four main parts, a descriptive part, a conceptual part, a part discussing two case studies and a conclusion. The first part is an accurate, useful and intriguing overview of EU legislative developments over the past thirty years. Arnbak distinguishes five "policy cycles", circling on critical infrastructures, cybercrime, personal data protection, telecommunications and E-signatures respectively. He further identifies three phases within those cycles. The initial surge of legislation in the 1990s was followed by standstill in the 2000s. Legislative traction re-emerged again in our decade, with proposals introduced and adopted in all five policy cycles. The book was finished in 2015, amid the third period of legislative development. Hence, the author could only speculate on the adoption of the General Data Protection Regulation in Spring 2016 and the Directive on the security of network and information systems that Summer. The two caused a profound change in EU private communications security law, but Arnbak could only discuss them in their draft form. That is of course not to the book's discredit – like in most academic works on the subject, the reader must reckon with the dynamism of cyber security regulation.

The descriptive Part 1 demonstrates the EU lawmaker's failure to design functioning regulations. Arnbak highlights instances of incoherence broadly, that is between policy cycles, and also narrowly, in the provisions of individual Directives and Regulations. The reader might wonder why those in charge of EU policy did not consult experts in the field to avoid this cacophony. One of the most striking examples is the scope of the telecommunication package. Telecom providers are included in this package, but digital service providers are not. Arnbak points out that a phone call is covered by these rules but a Skype call is not – it goes without saying that the two are, from the user's perspective, near-perfect substitutes.

In Part 2, the author discusses three conceptual perspectives: fundamental rights, system design and politics. The resultant insights are applied to digital signatures and cloud communication in Part 3. The lessons from these cases are summarized in Part 4 which leads to five recommendations.

In the discussion of fundamental rights, Arnbak is adamant that the EU lawmaker is under an obligation to ensure the security of private communications. The author thus approaches the research question within a normative framework. At this juncture, the book takes a more argumentative turn. For instance, the author is a strong advocate of private communications rights as "a first line of defence". The implication is that privacy should therefore be prioritized over other fundamental rights. Its priority is in his view a valid inference from the fundamental rights case law. However, the discussion could have benefitted from a more thorough discussion of alternative normative concerns. While the author does sometimes depart from his chosen normative perspective, societal values like national security are often neglected, a point which

he himself acknowledges. But there is still some tension between the singularity of the arguments and the book's stated aim to incorporate several perspectives and to provide an interdisciplinary perspective (p. 10). While system design and political perspectives are accorded some attention, there is only a cursory discussion of the potential trade-offs between secure communications and other values. But perfect security does not exist (p. 123) and legislation can hardly be expected to be a panacea. The EU lawmaker needs guidance on the stringency and boundaries of private communications legislation. Increased investments in private communication could reduce national security (targeted surveillance) or increase the (administrative) costs faced by businesses and individuals. It could even reduce aggregate social welfare. The latter may be traded for private communications protection. Nevertheless, to make informed policy choices, one must be cognizant of the social welfare reduction yielded by each legislative option.

The book is most convincing when it proposes technical legal improvements related to persistent market failures or new definitions in legislation. Both can arguably enhance social welfare. Specifically, the two case studies are accompanied by a valuable analysis of the relevant economic dynamics. Security economics provides profound insights into the effect of security investments, with special attention to externalities and information asymmetries. For instance, Arnbak points to solutions for "weakest link" and "too big to fail" issues in HTTPS communications which are likely to result in Pareto efficiency. Through its extensive discussion of HTTPS and secure cloud communications, this book raises awareness of the economic impact of legislation. The recommendations are oftentimes vital for the basic operation of the law.

Overall, the book's strongest point is the guidance on securing EU communications law, ranging from descriptive and normative stances to the specific. I would recommend this work to anyone tasked with improving private communications security law.

Bernold Nieuwesteeg
Rotterdam