Jean-François Blanchette: Burdens of Proof: Cryptographic Culture and Evidence Law in the Age of Electronic Documents The MIT Press: Cambridge and London, 2012. 264 pages.

In *Burdens of Proof*, Jean-François Blanchette examines the development of digital signatures, and the associated attempts to integrate them into evidentiary regimes. As such it is a welcome addition to our understanding of security technologies, given the somewhat triumphalist accounts of the development of digital signatures and their cryptographic underpinnings in the popular literature. It also chimes well with an emerging literature that is critical of cyber-utopianism and the hubris often encountered in discussions about the transformative power of the Internet.

Similar to the way written signatures are used to ensure the authenticity of paper documents, digital signatures are technologies that can be used to ensure the authenticity of electronic documents. This is achieved through the use of public-key cryptography. First proposed by Stanford computer scientists Whitfield Diffie and Martin Hellman in 1976, digital signatures have since been seen by many as crucial to the successful realization of electronic commerce, the paperless office, and more generally, the information society. However, integrating digital signatures into legal frameworks designed to consider written evidence has proved difficult. Similarly, other promised developments based on public-key cryptography, such as electronic cash, have largely failed to materialize. In *Burdens of Proof*, Blanchette aims to shed light on digital signatures' "failure to perform", and in doing so, provides one of the first sociological books to offer a detailed examination of modern cryptographic technologies.

Blanchette makes three overlapping arguments. Firstly, that the characterization of cryptography and digital signatures as fundamentally immaterial has made their translation into hardware and software artefacts problematic. Secondly, that attempts to mathematize certain areas of cryptography, with the aim of providing provable security, have marginalized areas of research that, although resistant to mathematization, can deliver a greater social impact. Thirdly, that the way in which cryptographers have modelled digital signatures has served to obscure the trade-offs inherent in producing cryptographic technologies that are to function in the real world.

Much of the evidence for these arguments is drawn from the attempts by the French legal system to integrate digital signatures into their evidentiary regime. Blanchette is particularly well placed to describe this, given that he was a member of a French Ministry of Justice task force charged with providing guidance about digital signatures to the French courts. Blanchette focuses on specific examples, such as the introduction of the *Réseau Elecronique NotariAL* (REAL) electronic notarial system. In this case, the models on which digital signatures were based, concerned as they were with highly technical or mathematical attacks, did not map well onto the primary requirements of the system, which included the physical presence of the notary, and long-term integrity and legibility lasting 100 years.

According to Blanchette, requirements like these evolved alongside the paper-based materials used to realize them. Although many have moved away from John Perry Barlow's 1996 claim that, in cyberspace, "… concepts of property, expression, identity, movement, and context do not apply", because "they are all based on matter, and there is no matter here", ideas about the immateriality of the digital persist (Barlow, 1996). However, Blanchette argues that, in the case of digital signatures, the belief that they occupy an immaterial world of pure information has only served to make requirements like physical presences harder to confront, whilst also obscuring some of the traditional security affordances of paper.

This isn't a long book, but it covers a lot of ground. As appears to be standard practice for books on cryptography, the early chapters are devoted to explaining some of the fundamental ideas that have shaped the history of cryptography. The techniques used to describe, say, the mechanics of a simple substitution cipher will be familiar to those who have read any of the many available technical primers. Nonetheless, Blanchette does a commendable job of introducing concepts that are not easily described in writing. Through his use of colourful examples, Blanchette convincingly shows that, throughout history, cryptography has been material, uncertain, and its success dependent on the context in which it was deployed. The Enigma Machine, one of the most well known implementations of cryptography, was a tangible piece of technology, and its downfall lay partly in the fact that it was so easy to use. Operators began to use it to encrypt routine communications, they became careless in their use of the machine, and this allowed Allied cryptanalysts to gain a foothold that eventually led to their ability to read Enigma-encrypted messages.

The focus is then narrowed from cryptography to digital signatures. We are brought up to date on how the field has developed, particularly in terms of how scientists and mathematicians conceptualized digital signatures, and how they modelled the problems and threats that they would encounter. Was the electronic document actually signed by the person it claims to have been signed by? Could it have been intercepted, modified, or signed by someone else? Blanchette claims that these questions were answered in particular ways. A one size fits all approach was adopted, and potential adversaries were endowed with the technical competences one would associate with intelligence agencies. The discrepancies surrounding materiality and context are cemented with Blanchette's description of how scientists grappled with the idea of provable security, and the epistemological status of various mathematical techniques for assessing algorithms. Towards the end of the book, we are introduced to some of the ways in which scientists have begun to engage with the problems surrounding mathematization and materiality in cryptography, and Blanchette makes a good case for continuing to think along these lines in the future.

This highlights a disconnect between theory and practice in cryptography. On this point, Blanchette's evidence is compelling and his claims are convincing. However, it is difficult to fully understand how scientists developed their models of how cryptography would be used without also understanding the institutional contexts in which they were working. Similarly, the public policy debates over the regulation and appropriate use of cryptography, sometimes referred to as the Crypto Wars, that occurred alongside much of this work should have been given a more prominent place in the descriptions. Blanchette stated that he did not want to revisit these debates, but I would argue that a significant portion of the work on cryptography from the 1990s onwards was done so with these debates

in mind, and is particularly relevant to claims made about how cryptography was modelled. Nonetheless, this is an engaging and nuanced account of the development of an increasingly important technology that has much to teach us about the relationships between science, technology and society.

References

Barlow. J.P. (1996) A Declaration of the Independence of Cyberspace [online] Available at: http://projects.eff.org/~barlow/Declaration-Final.html [Accessed 28 June 2013].

Richard Fletcher
University of Surrey
Guildford, UK
r.j.fletcher@surrey.ac.uk