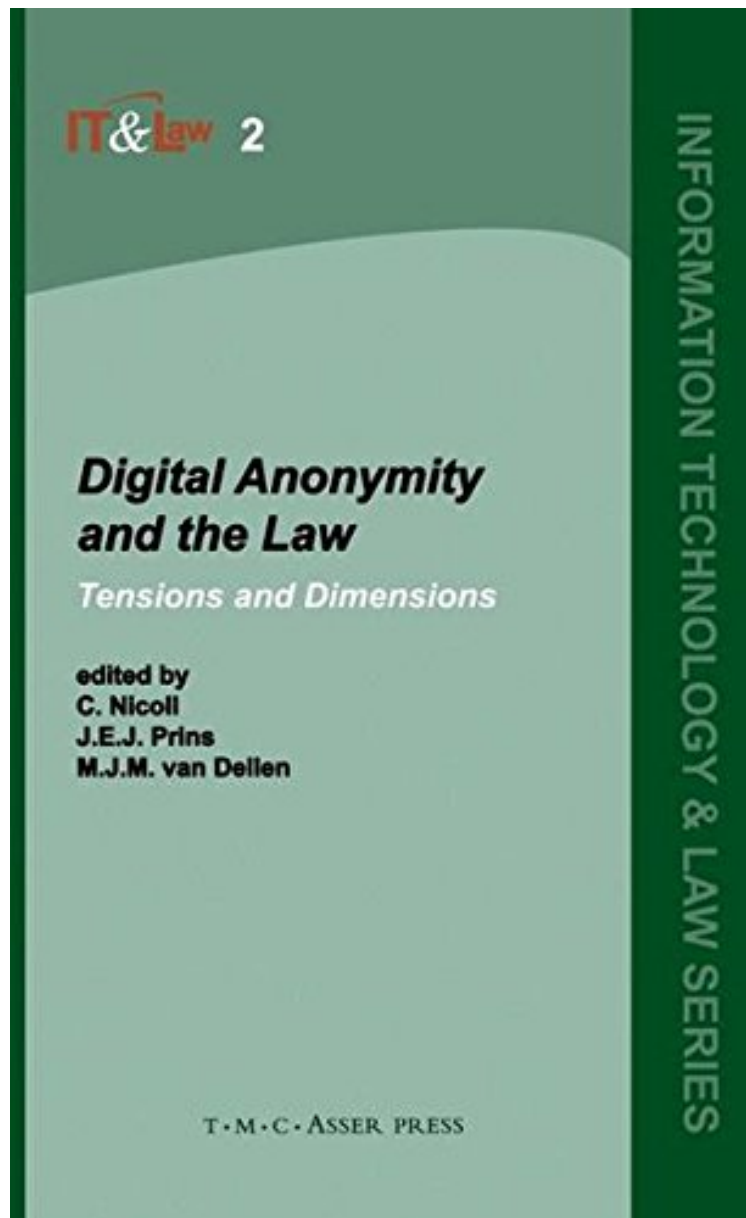


(Download pdf) Digital Anonymity and the Law: Tensions and Dimensions (Information Technology and Law Series)

Digital Anonymity and the Law: Tensions and Dimensions (Information Technology and Law Series)

From Brand: T.M.C. Asser Press
*ebooks | Download PDF | *ePub | DOC | audiobook*



[Download](#)

[Read Online](#)

#12351170 in Books T.M.C. Asser Press 2003-05-15 Original language: English PDF # 1 9.65 x .91 x 6.18l, 1.63 #File Name: 9067041564307 pages | File size: 57.Mb

From Brand: T.M.C. Asser Press : Digital Anonymity and the Law: Tensions and Dimensions (Information Technology and Law Series) before purchasing it in order to gage whether or not it would be worth my time, and all

praised Digital Anonymity and the Law: Tensions and Dimensions (Information Technology and Law Series):

10 of 10 people found the following review helpful. What anonymity? What law? By Kindle Customer I just received a copy and haven't read it cover-to-cover yet. I have, however, thumbed through several sections and am sorely disappointed. As an attorney, I find most egregious the lack of a case index (much less a statute index). Indeed, with the exception of Michael Froomkin's section, the book is largely devoid of cases and equally devoid of robust citation (whether in legal form, or otherwise). The remailer section does not describe how deployed remailer systems work in an even remotely correct way. The authors seem to confuse several different concepts and place remailers on the wrong network layer, too. They seem to miss how remailers actually provide anonymity. The onion routing section is equally vacuous, and would describe any of a half-dozen systems. The authors say "encrypt" when they mean "decrypt," and don't realize that stream-based protocols are handled with symmetric crypto. This is basic stuff. In addition, the only footnote to the onion routing section is a website, when there are plenty of published papers they could list instead. Also, why have the authors included mention of onion routers, without any mention of the vastly more interesting Freedom Network? For that matter, why did they spend a CHAPTER on JANUS as a "case study", but relegate Anonymizer to one third of a page and omit the Freedom Network entirely? Legal analysis of the Freedom Network is PRECISELY what I would expect to appear in a book titled "Digital Anonymity and the Law" and published in 2003. The book's preface refers to the "US Patriot Act" rather than USA PATRIOT or other correct citation. This might be acceptable in other texts, but this is the first page of a legal publication! On a whole, I'm not sure what the audience of this book is intended to be. It's certainly not attorneys practicing anonymity law! I am considerably less interested in reading this book cover-to-cover now. I will write an updated review if I can slog through it.

The right to anonymous exchange of information as well as anonymous communication is in an odd state of paradox. While the formal legal protection of this right appears at an all-time high, developments in both the public and private sector show a growing number of legal and especially technical means to undermine anonymity. The growing interest of people in using the Internet has had a key impact on the worldwide availability of personal information. Everyday life is evidence that technological advance provides numerous opportunities to trace and track people down. They fuel the commercial interests of persons and organisations who seek to know exactly who is accessing certain digital content in order to be able to charge for it. The pressure on anonymous communication has grown substantially after the 2001 terrorist attack on the World Trade Center and the subsequent new political climate. Although it is still difficult to oversee their exact implications, measures such as the US Patriot Act, the European Cybercrime Convention and the European Union rules on data retention may perhaps be only the very first signs that the exercise of the right to the anonymous exchange of information is under substantial pressure. These and other developments have fuelled the dialogue on the beliefs and values behind anonymous communication. Debates rage about how, by whom, and to what extent cyberspace anonymity should be controlled, for technological advance not only provides for new opportunities to trace and track people down.