Rule of Law Rhetoric in Encryption's 'Going Dark' Debate

Peter Alexander Earls Davis*

* Postdoctoral Research Fellow, Centre for Information and Innovation Law, University of Copenhagen. paed@jur.ku.dk.

Abstract

Encryption's 'going dark' debate concerns the availability and seamless use of strong forms of encryption to the general public, and its negative effects on law enforcement and intelligence agencies. In debating appropriate regulatory approaches, commentators typically reach for a privacy vs security heuristic: agencies tend to advance policies that privilege security over privacy, and their critics advance the opposite. However, critics of encryption have recently used 'rule of law' rhetoric to bolster arguments that more needs to be done to curb encryption's perceived harms. This paper discusses whether such invocations of the 'rule of law' are disingenuous political rhetoric, or are worthy of attention given understandings of the rule of law paradigm in present-day discourse.

1 Introduction[†]

As put by one pair of scholars, 'For government investigators, encryption adds an extra step: They must figure out a way to access the plaintext form of a suspect's encrypted data.'[1] The societal ramifications of this 'extra step' have proven substantial. Encryption, due to its deleterious effect on government investigations, presents one of the most confounding and incessant issues of today's information society.[2]

Debates around encryption can occur from many perspectives: amongst them technological, legal, political, economic, and ethical. One narrative advanced by encryption's sceptics is that encryption has a negative impact on societies otherwise governed by the rule of law. This paper seeks to challenge these assertions, by unpacking and then critically analysing claims made to this end.

This paper proceeds as follows. First, the following section offers a brief primer on the key contemporary debates around encryption, and the rough battle lines that have been drawn by key stakeholders. The third section analyses how rule of law rhetoric has entered debates, and identifies three types of rule of law arguments made by encryption's critics. The fourth section discusses the different possible meanings of the rule of law generally located by scholars, and analyses whether the three aforementioned arguments fall within these meanings. Through this analysis, it is argued that encryption's advocates, not its critics, are better justified in using the rule of law to advance their own normative claims.

[†] Work on this paper has been conducted at the University of Oslo under the aegis of the project 'Security in Internet Governance and Networks: Analysing the Law' (SIGNAL), funded by the Norwegian Research Council and UNINETT Norid AS. All URL references are cited as of the date indicated in the perma.cc link. Thanks are due to Lee Bygrave, Tobias Mahler, Ian Walden and Angela Daly for comments on an earlier version of this work. Nonetheless, the usual disclaimer applies.

[1] Orin Kerr and Bruce Schneier, 'Encryption Workarounds' (2018) 106 Georgetown Law Journal 989, 991.

[2] As Rozenshtein describes, encryption presents a 'wicked' problem: Alan Rozenshtein, 'Wicked Crypto' (2018) 9 UC Irvine Law Review 1181; see also Bert-Jaap Koops, *The Crypto Controversy: A Key Conflict in the Information Society* (Kluwer 1999).

2 Narratives in 'Going Dark' Discourse: Security vs Privacy

Encryption can frustrate the gathering of digital intelligence that is important to the protection of national security, and can stifle the collection of evidence to investigate and prosecute criminal activity. A problem often referred to as 'going dark' or 'going spotty',[3] contemporary encryption-related policy and legal debates centre around certain forms and use-contexts of encryption. In particular, the increased use of so-called 'warrant-proof'[4] encryption, made seamlessly available by multinational technology companies, has invoked the ire of law enforcement and intelligence agencies globally.[5] These agencies, and their evangelists, have routinely advocated for strong regulatory responses to ameliorate perceived harms enabled by such forms of encryption. Meta (but particularly its WhatsApp), Apple, and Google are arguably the prime targets of Western governments, given their significant market share in mobile devices and peer-to-peer communications.

Agencies and lawmakers have a vast menu of regulatory responses[6] from which to choose – or, at least attempt to enact and enforce. Options range from 'doing nothing'[7] to outright banning (problematic forms of) encryption[8] to ensure that agencies have access to intelligible information when needed.

Most regulatory proposals in this field attract sharp criticism; particularly those that are perceived to undermine the integrity of cryptosystems themselves. The most ferocious resistance comes from corporate and civil society actors, with individual privacy doubtless being the most cited concern.[9] Conversely, those championing more intrusive solutions point mainly to national security and

---

3 See Ian Walden, ''The Sky is Falling!' – Responses to the 'Going Dark' problem' (2018) 34 Computer Law & Security Review 901; Thiago Moraes, 'Sparkling Lights in the Going Dark: Legal Safeguards for Law Enforcement's Encryption Circumvention Measures' (2020) 1 European Data Protection Law Review 15.

4 William Barr, 'Attorney General Delivers Remarks at the Lawful Access Summit' (*Department of Justice*, 4 October 2019) <https://www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-remarks-lawful-access-summit> [https://perma.cc/UH8N-4MAK].

5 This paper focuses on Western jurisdictions, particularly the United States, European Union, and Australia. However, on the international dimensions of this issue, see Ryan Hal Budish, Herbert Burkert and Urs Gasser, *Encryption Policy and Its International Impacts: A Framework for Understanding Extraterritorial Ripple Effects* (Hoover Institution Aegis Series, 2018); Eric Manpearl, 'The International Front of the Going Dark Debate' (2019) 22 Virginia Journal of Law & Technology 158; James Lewis, Denise Zheng and William Carter, *The Effect of Encryption on Lawful Access to Communications and Data* (2017).

6 For a selection, see Walden, ''The Sky is Falling!' – Responses to the 'Going Dark' problem'; Andreas Kuehn and Bruce McConnell, *Encryption Policy in Democratic Regimes: Finding Convergent Paths and Balanced Solutions* (EastWest Institute Policy Report, 2018).

7 Koops, *The Crypto Controversy: A Key Conflict in the Information Society*, 233ff.

8 Walden, ''The Sky is Falling!' – Responses to the 'Going Dark' problem', 902.

9 For a critical analysis, see Seda Gürses, Arun Kundnani and Joris Van Hoboken, 'Crypto and empire: the contradictions of counter-surveillance advocacy' (2016) 38 Media, Culture & Society 576; see further Matthias Schulze, 'Clipper Meets Apple vs. FBI—A Comparison of the Cryptography Discourses from 1993 and 2016' (2017) 5 Media and Communication 54; Adam Moore, 'Privacy and the Encryption Debate' (2000) 12 Knowledge, Technology & Policy 72.

public safety as justifying incursions into individual privacy. Thus, in assessing the desirability of regulatory (in)action in this space, it is common[10] for participants to reach for a dichotomy: of privacy on one hand, and security on the other. The preferable policy response, it is said, is one that appropriately balances these values, which are cast as being in competition with one another.[11]

If one (arguably falsely[12]) perceives of the encryption debate as being between two polarised sides – one pro-encryption, and one pro-agency – then there are signs that neither is satisfied with the privacy vs security framing. Commentators that tend to lean pro-encryption have identified many issues with perceiving the 'going dark' debate – and broader debates about surveillance powers – through such a binary lens.[13] To briefly summarise, there is concern that this framing is misleading, overly reductive, or even contradictory given the importance of sound (cyber-)security for individual privacy and national security.[14]

The pro-agency side's rationale for looking beyond the dichotomy is somewhat different. With the threat of Islamic terrorism receding in most of the Western world,[15] intrusions into fundamental rights, such as privacy, in the name

---

[10] Rozenshtein, for instance, refers to the 'standard framing of encryption as a "privacy vs. security" issue': Alan Rozenshtein, 'Surveillance Intermediaries' (2018) 70 Stanford Law Review 99, 137. See further Jacob Zarefsky, 'The Precarious Balance between National Security and Individual Privacy: Data Encryption in the Twenty-First Century' (2021) 23 Tulane Journal of Technology & Intellectual Property 179; Richard Spinello, 'The ethical consequences of "going dark"' (2021) 30 Business Ethics, the Environment & Responsibility 116, 117.

[11] E.g. EU Council Resolution on Encryption – Security through encryption and security despite encryption (Resolution 13084/1/20 REV 1) at 3-4, which speaks of '[s]triking the right balance', mentioning the importance of '[p]rotecting the privacy and security of communications through encryption and at the same time upholding the possibility for competent authorities in the area of security and criminal justice'.

[12] The Carnegie Working Group on Encryption in a 2019 report warns of 'absolutist positions not actually held by serious participants [of the 'going dark' debate], but sometimes used as caricatures of opponents': Carnegie Encryption Working Group, *Moving the Encryption Policy Conversation Forward* (Carnegie Endowment for International Peace Working Paper, 2019), 6.

[13] See e.g. Schulze, 'Clipper Meets Apple vs. FBI—A Comparison of the Cryptography Discourses from 1993 and 2016', 59; Monique Mann and others, 'The Limits of (Digital) Constitutionalism: Exploring the Privacy-Security (Im)balance in Australia' (2018) 80 International Communication Gazette 369, 373ff; Paul Bernal, *The Internet, Warts and All: Free Speech, Privacy and Truth*, vol 48 (Cambridge Intellectual Property and Information Law, Cambridge University Press 2018), 170; Mireille Hildebrandt, 'Balance or Trade-off? Online Security Technologies and Fundamental Rights' (2013) 26 Philosophy & Technology 357; Encryption Working Group, *Moving the Encryption Policy Conversation Forward*; Dave Weinstein, 'Privacy vs. Security: It's a False Dilemma' (*Wall Street Journal*, 6 October 2019) <https://www.wsj.com/articles/privacy-vs-security-its-a-false-dilemma-11570389477> [https://perma.cc/GJ53-R277].

[14] Mann and others, 'The Limits of (Digital) Constitutionalism: Exploring the Privacy-Security (Im)balance in Australia', 377.

[15] See e.g. Lewis Herrington, 'British Islamic extremist terrorism: the declining significance of Al–Qaeda and Pakistan' (2015) 91 International Affairs 17; Institute for Economics & Peace, *Global Terrorism Index 2020: Measuring the Impact of Terrorism* (National Consortium for the Study of Terrorism and Responses to Terrorism, 2020).

of 'security' presents a less compelling narrative than it once did. Whilst pro-agency advocates do continue to cite security concerns,[16] these are often raised in tandem with other grounds like child safety (typically in the context of preventing the proliferation of child sexual abuse material).[17] As elaborated below, the rule of law offers a further rhetorical alternative.

3 Rule of Law Rhetoric in 'Going Dark' Discourse

Having briefly outlined the contours of the contemporary 'going dark' debate, this section analyses how pro-agency advocates have used rule of law rhetoric in public discourse. For illustrative purposes, these are split into three species of argument (that exhibit some conceptual overlap). The cogency of these three types of claims are discussed in the section that follows.

Conveniently, each of these three claims are made – albeit somewhat implicitly, and imprecisely – by then-FBI Director James Comey in a 2014 speech outlining the agency's concern with encryption. Comey's speech took place in October 2014 – tellingly, a month after Apple and Google announced stronger encryption in their iOS and Android operating systems, and a month before WhatsApp did similarly. One key remark was as follows:

> I hope you know that I'm a huge believer in the rule of law. But I also believe that no one in this country should be above or beyond the law. There should be no law-free zone in this country. I like and believe very much that we need to follow the letter of the law to examine the contents of someone's closet or someone's cell phone. But the notion that the marketplace could create something that would prevent that closet from ever being opened, even with a properly obtained court order, makes no sense to me.
>
> I think it's time to ask: Where are we, as a society? Are we no longer a country governed by the rule of law, where no one is above or beyond that law? Are we so

---

[16] In the EU, see e.g. Council of the European Union, 'Joint statement by the EU home affairs ministers on the recent terrorist attacks in Europe' (*EU Council*, 13 November 2020) <https://www.consilium.europa.eu/en/press/press-releases/2020/11/13/joint-statement-by-the-eu-home-affairs-ministers-on-the-recent-terrorist-attacks-in-europe/> [https://perma.cc/T6UR-8QFT]; in Australia, see Keiran Hardy, 'Australia's encryption laws: practical need or political strategy?' (2020) 9 Internet Policy Review 1. On encryption's utility to terrorists, particularly Islamic terrorists, see Robert Graham, *How Terrorists Use Encryption* (CTC Sentinel, 2016); Lewis, Zheng and Carter, *The Effect of Encryption on Lawful Access to Communications and Data*, iv; Christopher Ahlberg, 'How Al-Qaeda Uses Encryption Post-Snowden (Part 1)' (*Recorded Future*, 8 May 2014) <https://www.recordedfuture.com/al-qaeda-encryption-technology-part-1/> [https://perma.cc/L89W-WAGT].

[17] On the US, see Riana Pfefferkorn, 'Banning Strong Encryption Does Not Mean Catching Criminals. It Only Makes You Less Safe from Them.' (*Stanford*, 24 November 2019) <http://cyberlaw.stanford.edu/blog/2019/11/banning-strong-encryption-does-not-mean-catching-criminals-it-only-makes-you-less-safe> [https://perma.cc/Q4AC-YT99]: '… after years of terrorism being the favored rationale for their endless war against strong encryption, law enforcement agencies in the U.S. (and other countries) suddenly changed their public-relations messaging to focus almost exclusively on CSAM.'; On the EU, see Maria Koomen, *The Encryption Debate in the European Union: 2021 Update* (Carnegie Endowment for International Peace Working Paper, 2021).

> mistrustful of government – and of law enforcement – that we are willing to let bad guys walk away ... willing to leave victims in search of justice?

The first observable rule of law argument considered derives from a concern that lawfully procured legal instruments like warrants and subpoenas may sometimes be rendered useless due to the presence of encryption. The fact that encryption can circumvent or overcome legitimately enacted law (or enable those using it to be 'above the law'[18]) is therefore said to be a threat to the rule of law.

The second is that encryption has a deleterious effect on law enforcement or intelligence agency investigations, which goes against understandings of justice. Justice, under this argument, is a key component of, or at least inextricable from, the rule of law.

It is thirdly argued that agency-stifling – or 'warrant-proof' – encryption is facilitated and promoted by certain technology companies operating in their own self-interest. This is the 'marketplace' referred to by Comey above. Decisions about how much information should be accessible to agencies are to be properly made by democratically elected officials or other competent authorities – and not private corporations that are answerable only to shareholders. The fact that companies like Apple, Google, and Facebook have reduced agencies' capabilities through, *inter alia*, encryption, especially post-Snowden,[19] is said to be problematic from a rule of law perspective.

A fourth species of argument can also be observed at the beginning of Comey's above-mentioned remark – though from the opposing pro-encryption, or perhaps pro-privacy/anti-surveillance, perspective. Comey pays credence to the rule of law issues that tend to arise[20] in the context of national security, surveillance, intelligence and so on – and which were fresh in mind post-Snowden[21] at the time of the speech. Encryption has been heralded by some[22] as a partial antidote to overzealous agencies which do not observe the rule of law.[23]

---

18 Unknown Author, 'Intelligence Committee Leaders Release Discussion Draft of Encryption Bill - Press Releases - United States Senator for California' (*Dianne Feinstein*, 13 April 2016) <https://www.feinstein.senate.gov/public/index.cfm/2016/4/intelligence-committee-leaders-release-discussion-draft-of-encryption-legislation> [https://perma.cc/HP9D-Z863].

19 For a thorough account of this phenomenon, see Rozenshtein, 'Surveillance Intermediaries'.

20 E.g. Lord Tom Bingham, 'The Rule of Law' (2007) 66 The Cambridge Law Journal 67, 69, pointing to rule of law concerns with the operation of opaque government powers.

21 See e.g. Lisa Austin, 'Surveillance and the Rule of Law' (2015) 13 Surveillance & Society 295; Lisa Austin, 'Lawful Illegality: What Snowden Has taught Us about the Legal Infrastructure of the Surveillance State' in Michael Geist and Wesley Wark (eds), *Law, Privacy and Surveillance in Canada in the Post-Snowden Era* (University of Ottawa Press 2014) 103-125; Ian Warren, Monique Mann and Adam Molnar, 'Lawful illegality: Authorizing extraterritorial police surveillance' (2020) 18 Surveillance & Society 357.

22 As put by Heiser, Bennett Moses and Teague, 'encryption limits the power of security agencies': Gernot Heiser, Lyria Bennett Moses and Vanessa Teague, 'ACIC thinks there are no legitimate uses of encryption. They're wrong, and here's why it matters' (*UNSW*, 19 May 2021) <https://www.unsw.edu.au/news/2021/05/acic-thinks-there-are-no-legitimate-uses-of-encryption--they-re-> [https://perma.cc/U2BC-DJJ7].

23 See further Mann and others, 'The Limits of (Digital) Constitutionalism: Exploring the Privacy-Security (Im)balance in Australia'; Monique Mann, Angela Daly and Adam Molnar,

This counter-perspective is considered throughout section 4 of this paper, in providing opposition to the pro-agency side's three main arguments.

3.1 Encryption as a Threat to (the Rule of) Law

There is little doubt that encryption is capable of preventing an agency from gathering intelligible evidence or intelligence. The classic example cited in contemporary 'going dark' discourse is Apple's refusal – or perhaps self-imposed inability[24] – to help the FBI decrypt a suspected terrorist's iPhone after the San Bernardino shooting in 2016.[25] A more direct example can be found in the blog of encrypted messaging company Signal. On at least two occasions, Signal has published responses to subpoenas served upon it, in which they boast of the paucity of user data they hold due to the design of their products (and in particular their chosen provision of encryption).[26]

These instances certainly suggest a 'gap between authority and capability'[27] due to encryption. But how does this present a rule of law issue? Whilst Comey's speech does not directly argue that it does, others on the pro-agency side have. The Australian experience in the field provides an apt example. In 2017, preceding a controversial legislative package on the topic,[28] then-Australian Prime Minister Malcolm Turnbull held a press conference centred on the rule of law and encryption. In it, he expressed concern 'about the challenges that we face in ensuring that the rule of law applies online as well as offline',[29] elaborating that '[w]hat we're talking about is the rule of law continuing to

---

'Regulatory arbitrage and transnational surveillance: Australia's extraterritorial assistance to access encrypted communications' (2020) 9 Internet Policy Review 1.

[24] See below at 3.3.

[25] For in-depth legal and factual analysis on-point, see Justin Hurwitz, 'Encryption.Congress mod (Apple + CALEA)' (2017) 30 Harvard Journal of Law & Technology 355; Steven Morrison, 'Breaking iPhones under CALEA and the All Writs Act: Why the Government Was (Mostly) Right' (2016) 38 Cardozo Law Review 2039.

[26] Signal, 'Grand jury subpoena for Signal user data, Eastern District of Virginia' (*Signal Blog*, 4 October 2016) <https://signal.org/bigbrother/eastern-virginia-grand-jury/> [https://perma.cc/S4UV-8DHP]; Signal, 'Grand jury subpoena for Signal user data, Central District of California' (*Signal Blog*, 27 April 2021) <https://signal.org/bigbrother/central-california-grand-jury/> [https://perma.cc/UE2L-6TNU].

[27] As put by then FBI General Counsel in 2011: Valerie Caproni, 'Going Dark: Lawful Electronic Surveillance in the Face of New Technologies' (*FBI*, 17 February 2011) <https://archives.fbi.gov/archives/news/testimony/going-dark-lawful-electronic-surveillance-in-the-face-of-new-technologies> [https://perma.cc/7FUW-GXDJ].

[28] In particular, the amendments arising from the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth). For a primer, see Arthur Kopsias, '"Going dark": the unprecedented government measures to access encrypted data' (2019) Law Society of NSW Journal 74; Peter Davis, 'Decrypting Australia's 'Anti-Encryption' legislation: The meaning and effect of the 'systemic weakness' limitation' (2022) 44 Computer Law & Security Review 105659.

[29] Malcolm Turnbull, 'Press Conference with Attorney-General and Acting Commissioner of the AFP' (*Malcolm Turnbull*, 14 July 2017) <https://www.malcolmturnbull.com.au/media/press-conference-with-attorney-general-and-acting-commissioner-of-the-afp-s> [https://perma.cc/WDZ8-LEDJ].

prevail in the online world as it has in the past… in the world when telecoms were not encrypted, were not end-to-end encrypted.'[30] When pressed by a journalist on how the legislative regime might function given the mathematical realities of encryption (a common refrain from the pro-encryption side[31]), Turnbull infamously[32] responded that 'the laws of mathematics are very commendable but the only law that applies in Australia is the law of Australia.'[33]

The central notion called upon is that encryption is itself a threat to the rule of law, as an instrument that frustrates lawful intelligence and evidence gathering. Further propositions that encryption enables the creation of 'safe spaces'[34] for criminal activity, or '"law-free zones" insulated from legitimate scrutiny',[35] follow along similar lines.

3.2 Encryption as an Affront to Justice

The second type of claim goes one step further than that just discussed. Not only, is it argued, does user-controlled encryption frustrate otherwise lawful access to information, but that this, in turn, is repugnant to entrenched notions such as 'justice and liberty [which] depend upon the rule of law'.[36] This is because encryption 'significantly impairs, if not entirely prevents, investigations involving violent crime, drug trafficking, child exploitation, cybercrime, and domestic and international terrorism',[37] resulting in justice not being done to the perpetrators, and received in kind by their victims and society at large.

---

30 Ibid.

31 See e.g. Harold Abelson and others, 'Keys Under Doormats: Mandating Insecurity by Requiring Government Access to all Data and Communications' (2015) 1 Journal of Cybersecurity 69.

32 Mann and others, 'The Limits of (Digital) Constitutionalism: Exploring the Privacy-Security (Im)balance in Australia', 7.

33 Turnbull, 'Press Conference with Attorney-General and Acting Commissioner of the AFP' <https://www.malcolmturnbull.com.au/media/press-conference-with-attorney-general-and-acting-commissioner-of-the-afp-s>

34 Glyn Moody, 'Cameron reaffirms there will be no safe spaces from UK government snooping' (*Ars Technica*, 1 July 2015) <https://arstechnica.com/tech-policy/2015/07/cameron-reaffirms-there-will-be-no-safe-spaces-from-uk-government-snooping/> [https://perma.cc/LTC4-XV9Z].

35 William Barr, 'Attorney General William P. Barr Delivers Keynote Address at the International Conference on Cyber Security' (*United States Department of Justice,* 23 July 2019) <https://www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-keynote-address-international-conference-cyber> [https://perma.cc/FJR2-DN6H]; see also James Comey, 'Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?' (*FBI*, 16 October 2014) <https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course> [https://perma.cc/DB4Q-JL3Y].

36 Ryan Patrick, 'Houston Chronicle Op-Ed: Encryption lets sexual predators escape the law' (*Department of Justice*, 20 December 2019) <https://www.justice.gov/archives/doj/blog/houston-chronicle-op-ed-encryption-lets-sexual-predators-escape-law> [https://perma.cc/HB9Z-NTMN].

37 Ibid.

Comey's earlier quote raises this argument explicitly. Academic commentators have made similar claims. Koops, writing on the 'Crypto Controversy' 1999,[38] interpreted – without much in the way of justification – the rule of law to mean 'the right to freedom from crime'.[39] Koops reasoned that '[t]he rule of law means, first, that a society should try to prevent crimes, and, second, that, committed crimes should be redressed, usually by prosecuting their perpetrators.'[40]

Koops' point resonates with other commentators' concerns of law enforcement's ability to carry out their duties effectively. Bay, writing about the San Bernardino iPhone saga through Rawlsian principles, in which 'rule of law is an important component in Rawls' well-ordered society', remarks that 'unbreakable cryptography… would be an obstruction of justice in such a society, as it is indisputable that encryption that is unbreakable by law enforcement operatives is a hindrance to the operatives' abilities to gather information.'[41] Bay concludes that 'unbreakable encryption', put through a Rawlsian lens, would be 'socially uncooperative and a hindrance of justice to allow it', in spite of encryption otherwise being 'a valid, useful and perhaps even necessary tool to protect privacy'.

3.3 Technology Companies as a Rule of Law Threat

The third claim focuses on the culpability of technology companies, particularly 'Big Tech', in their provision of 'warrant-proof' encryption to their end-users. The predominant focus of today's 'going dark' debate is arguably somewhat narrower than the existence and use of encryption *per se*. Rather, agency angst is mainly directed towards the post-Snowden tendency of technology companies, who provide a significant portion of Western agencies' surveillance capabilities,[42] to design their products to be unamenable to government search or surveillance.[43]

In its suit against Apple following the San Bernardino terrorist attack mentioned above, the FBI[44] argued that, '[t]he rule of law does not repose that

---

[38] Koops, *The Crypto Controversy: A Key Conflict in the Information Society*. Note that the 'Crypto Wars' of the 1990s concerned a rather different socio-technical context than encryption-related debates today. See further Danielle Kehl, Andi Wilson and Kevin Bankston, *Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s* (2015); Craig Jarvis, *Crypto Wars: The Fight for Privacy in the Digital Age: A Political History of Digital Encryption* (CRC Press 2020).

[39] Koops, *The Crypto Controversy: A Key Conflict in the Information Society*, 120.

[40] Ibid, 121.

[41] Morten Bay, 'The ethics of unbreakable encryption: Rawlsian privacy and the San Bernardino iPhone' (2017) 22 First Monday 1.

[42] Rozenshtein, 'Surveillance Intermediaries'.

[43] On this dynamic, see ibid; Kristen Eichensehr, 'Digital Switzerlands' (2019) 167 University of Pennsylvania Law Review 665.

[44] Or, more accurately, the US government: Morrison, 'Breaking iPhones under CALEA and the All Writs Act: Why the Government Was (Mostly) Right'.

power in a single corporation, no matter how successful it has been in selling its products',[45] and that 'Apple has attempted to design and market its products to allow technology, rather than the law, to control access to data which has been found by this Court to be warranted for an important investigation.'[46] Hurwitz later commented that 'law enforcement is effectively beholden to the past and present design decisions of manufacturers and service operators… [which] could be construed as an inappropriate usurpation of and interference with the legal authority vested in law enforcement.'[47] In this way, technology companies deliberately use encryption to usurp the rule of law. This strategy is labelled by Rozenshtein as '*technological unilateralism*: making technological changes to their systems irrespective of (if not intentionally adverse to) the government's preferences.'[48]

The rule of law claim is therefore one of legitimacy[49] – should 'Big Tech' have the power to decide what information is available and intelligible to agencies? Those on the pro-agency side think they should not, as a report from the Manhattan District Attorney's office makes plain:

> Big Tech should not be the entity to regulate Big Tech. Rather, Congress, comprised of democratically elected officials, "must determine the balance in our society between personal privacy and public safety."[50]

A discussion draft bill in the federal US Senate further illustrates this claim, though in a (draft) legal instrument. Senators Burr and Feinstein's bipartisan bill, entitled the *Compliance with Court Orders Act of 2016*[51] placed tech companies' role worsening agencies' surveillance capabilities explicitly in rule of law terms. Section 2 of the draft pronounced in a 'sense of'[52] provision, *inter alia*, that:

> It is the sense of Congress that—
>
> (1) no person or entity is above the law;

---

45 FBI Motion to Compel Apple to Comply with the Court's February 16, 2016 Order (Feb. 19, 2016), 35.

46 Ibid, 6.

47 Hurwitz, 'Encryption.Congress mod (Apple + CALEA)', 422.

48 Rozenshtein, 'Surveillance Intermediaries', 134.

49 By legitimacy, it is herein meant the 'justification of authority' from a normative perspective: Rolf Weber, *Shaping Internet Governance: Regulatory Challenges*, vol 46 (Springer Science & Business Media 2010), 109.

50 Manhattan District Attorney's Office, *Smartphone Encryption and Public Safety: An Update to the November 2018 Report* (2019), 20, referring to Cyrus Jr Vance, Jackie Lacey and Bonnie Dumanis, 'Op-Ed: Congress can put iPhones back within reach of law enforcement' (*Los Angeles Times*, 11 May 2016) <https://www.latimes.com/opinion/op-ed/la-oe-vance-congress-act-on-iphones-20160511-story.html> [https://perma.cc/J4FE-FEML].

51 *Compliance with Court Orders Act of 2016*, 114th Congress (discussion draft 2016).

52 'Sense of' provisions are not binding in US law. See Paul Rundquist, "*Sense of" Resolutions and Provisions* (Congressional Research Service, 2019).

> (2) economic growth, prosperity, security, stability, and liberty require adherence to the rule of law; …
>
> (4) all providers of communications services and products (including software) should protect the privacy of United States persons through implementation of appropriate data security and still respect the rule of law and comply with all legal requirements and court orders;
>
> (5) to uphold both the rule of law and protect the interests and security of the United States, all persons receiving an authorized judicial order for information or data must provide, in a timely manner, responsive, intelligible information or data, or appropriate technical assistance to obtain such information or data…

Given this bill was released in the midst of the aforementioned Apple v FBI dispute, it is not difficult to see this provision as aimed at Apple, and other technology companies that adopt similar agency-stifling practices with regards to encryption. The bill expressly calls upon them to facilitate the rule of law – without specifying what is meant by that term – and states that any of their commercial interests must yield to rule of law concerns.

4 Rule of Law Rhetoric in Encryption Discourse: Cogent or Deceitful?

It may be tempting to dismiss the above invocations of the rule of law as 'little more than "Hooray for our side!"'[53] The rule of law could be accused, in the above context, of being 'just an empty slogan, useful perhaps as decoration for whatever else one wants to assert into a political dispute, but incapable of driving one's argument much further forward than the argument could have driven on its own.'[54] As put by Tamanaha, 'the rule of law is analogous to the notion of the "good," in the sense that everyone is for it, but have contrasting convictions about what it is.'[55] What is the point, then, of taking the pro-agency side's claims as more than just vapid political rhetoric?

To avoid confronting the esoteric question of rule of law's ultimate utility,[56] it suffices to claim that those wishing to call upon the rule of law for political

---

[53] Jeremy Waldron, 'Is the Rule of Law an Essentially Contested Concept (in Florida)?' (2002) 21 Law and Philosophy 137, 139.

[54] Ibid, 139; referring to Judith Shklar, 'Political Theory and The Rule of Law' in Allan Hutcheson and Patrick Monahan (eds), *The Rule of Law: Ideal or Ideology* (Carswell 1987), 1.

[55] Brian Tamanaha, *On the Rule of Law: History, Politics, Theory* (Cambridge University Press 2004), 3. It is worth mentioning that the 'rule of law' discussed here is distinct from its use as an enforceable legal doctrine: see further Jeffrey Goldsworthy, 'Legislative sovereignty and the rule of law' in Jeffrey Goldsworthy (ed), *Parliamentary Sovereignty: Contemporary Debates* (Cambridge Studies in Constitutional Law, Cambridge University Press 2010) 57-78, 58-63.

[56] A question that has been extensively debated: see e.g. Shklar, 'Political Theory and The Rule of Law'; Bingham, 'The Rule of Law'; Jeremy Waldron, 'The Rule of Law as an Essentially Contested Concept' (2021) NYU School of Law, Public Law Research Paper No 21-15 1.

action do so because it *does* mean something. And, those same groups or individuals should be open to challenge on their use of it.

Nevertheless, even if one assumes that the rule of law is worth more than mere 'ruling-class chatter',[57] Tamanaha's abovementioned quote raises a further question: what does the rule of law mean? In this vein, the rule of law is arguably an 'essentially contested concept'[58] – 'said to be so value-laden that no amount of argument or evidence can ever lead to agreement on a single version as the "correct or standard use".'[59]

One means of resolving this conundrum would be to adopt a particular understanding of the rule of law as the 'correct' one, and assess whether the three species of argument identified above abide by that understanding. However, the point of this paper is to analyse the cogency of rule of law claims in 'going dark' discourse; not the cogency of a particular conception of the rule of law. Therefore, it serves to canvas the various types of rule of law conceptions and ask which, if any, those on the pro-agency side are pointing to. From there, it is possible to assess the merits of these claims, including whether there are inconsistencies or contradictions in usage of the rule of law paradigm.

4.1 Thin to Thick: Systematisations of the Rule of Law

The otherwise cumbersome task of wading through the myriad disputed meanings of the rule of law is made easier by scholars that have categorised and systematised different understandings of the paradigm. Those devoted to researching these different rule of law conceptions generally identify two types of approaches: 'thin' and 'thick'. Put simply,[60] thin approaches are positivist, minimalist, and focus on form rather than content. Thick approaches generally include thin components, but further include substantive aspects, and are oriented towards notions of justice.[61] Although often cast as a dichotomy, thin and thick conceptions are perhaps better understood as a spectrum or 'progression',[62] with scholars including Raz and Dicey at the thinner end,[63] and Dworkin and Bingham towards thicker.[64] It is generally agreed[65] that the thinnest possible conception is rule *by* law: 'that whatever a government does, it should

---

57 Shklar, 'Political Theory and The Rule of Law', 1.

58 Waldron, 'Is the Rule of Law an Essentially Contested Concept (in Florida)?'.

59 David Baldwin, 'The Concept of Security' (1997) 23 Review of International Studies 5, 10.

60 For an elaboration, see Paul Craig, 'Formal and substantive conceptions of the rule of law: an analytical framework' (1997) Public Law 467; Simon Chesterman, 'An International Rule of Law?' (2008) 56 The American Journal of Comparative Law 331, 340-342.

61 Chesterman, 'An International Rule of Law?', 347.

62 Tamanaha, *On the Rule of Law: History, Politics, Theory*, 91.

63 Craig, 'Formal and substantive conceptions of the rule of law: an analytical framework'.

64 Chesterman, 'An International Rule of Law?', 341.

65 Tamanaha, *On the Rule of Law: History, Politics, Theory*, 92.

do through laws.'[66] Conversely, the thickest notions include what 'might be roughly categorized under the label "social welfare rights."'[67]

Møller and Skaaning,[68] building off existing systemisations of rule of law concepts,[69] develop a one-dimensional hierarchy that identifies six different rule of law notions and ranks them from thinnest to thickest. One of Møller and Skaanings' stated purposes of building the hierarchy is to 'allow scholars carrying out theoretical and empirical analyses to distinguish between thinner and thicker definitions of the rule of law and make more conscious choices when selecting between them,'[70] Hence, the remainder of this section attempts to place the three species rule of law claims in 'going dark' discourse within this hierarchy. This analytical approach is also envisaged by Carlin: 'rule-of-law scholars can operationalise a conceptual definition of rule of law and examine how closely cases match an ideal type.'[71]

Møller and Skaaning's hierarchy is chosen over other systematisations for its relative elegance and simplicity, though it must be said that it is broadly similar to others.[72] The hierarchy is reproduced below.

Concept	**Defining Attributes**
Rule by law	Power exercised via positive law
Formal legality	+ General, public, prospective, certain, equally applied
Safeguarded rule of law	+ Control (checks + balances)
Liberal rule of law	+ Negative content (liberal rights)
Democratic rule of law	+ Consent (lawmakers chosen by competitive elections)
Social democratic rule of law	+ Positive content (social rights)

Table 1: Hierarchy of Rule of Law Concepts by Møller and Skaaning

Each 'concept' is inclusive of the previous concepts, as indicated by the + in the 'defining attributes'. For instance, the concept of formal legality includes

---

66 Noel Reynolds, 'Grounding the Rule of Law' (1989) 2 Ratio Juris 1, 3.

67 Tamanaha, *On the Rule of Law: History, Politics, Theory*, 112.

68 Jørgen Møller and Svend-Erik Skaaning, 'Systematizing Thin and Thick Conceptions of the Rule of Law' (2012) 33 The Justice System Journal 136.

69 Ibid, 132-4. Møller and Skaaning's hierarchy is similar to that developed by Tamanaha in Tamanaha, *On the Rule of Law: History, Politics, Theory*, 92.

70 Møller and Skaaning, 'Systematizing Thin and Thick Conceptions of the Rule of Law', 150.

71 Ryan Carlin, 'Rule-of-Law Typologies in Contemporary Societies' (2012) 33 The Justice System Journal 154, 154.

72 Møller and Skaaning, 'Systematizing Thin and Thick Conceptions of the Rule of Law', 143-5.

rule by law; democratic rule of law includes liberal rule of law and so on. The content of these concepts is elaborated below, where each concept is deliberated upon sequentially.

4.2 Rule by Law

Power exercised via positive law

The 'thinnest' conception of rule of law is rule *by* law. Waldron describes rule by law as '[t]he idea… that the law should stand above every powerful person and agency in the land'.[73] The antithesis of rule by law is rule by man, 'implying power exercised at the whim of an absolute ruler'.[74] By this understanding, rule by law and, hence, rule *of* law, acts as a formal constraint on government power, and government power alone. Taken in this way, rule by law has only little relevance to the 'going dark' debate – it might only become relevant where a government actor purports to apply their power in a capricious and arbitrary manner to, for instance, force a provider or end-user to decrypt information in the absence of clear legal authority.[75]

Beyond this outcome, adherents to the rule of law's narrowest conception would find little force in arguments that the 'going dark' debate is a rule of law problem. The conduct of private actors (e.g. tech companies), the existence of insentient technologies (e.g. encryption, or mathematics), and even the apparent unbridled criminal conduct caused by them, simply does not figure in the rule of law paradigm. As a natural consequence of its historical provenance, the rule of law typically pertains to limits on the power of the government, not external forces that affect its ability to govern.[76] Arguments that private citizens,[77]

---

[73] Jeremy Waldron, 'The Rule of Law (Stanford Encyclopedia of Philosophy)' (*Stanford Plato*, 22 June 2016) <https://plato.stanford.edu/entries/rule-of-law/#RuleLawRuleLaw> [https://perma.cc/4GLJ-UXEV].

[74] Chesterman, 'An International Rule of Law?', 333.

[75] A version of this argument was made by Apple's legal team in their 2016 case with the FBI, where the former argued that the FBI lacked the requisite legal mandate to force the decryption of the suspect's iPhone. In particular, Apple stated that the 'Court should reject [the FBI's] request, because the All Writs Act does not authorize such relief, and the Constitution forbids it': *In the Matter of The Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203*, Apple Inc.'s Reply to Government's Opposition to Apple Inc. Motion To Vacate Order Compelling Apple Inc. to Assist Agents in Search, 15 March 2016, 8.

[76] As put by Raz, 'in political and legal theory [the rule of law] has come to be read in a narrower sense, that the government shall be ruled by the law and subject to it.' Joseph Raz, 'The Rule of Law and its Virtue' in Joseph Raz (ed), *The Authority of Law: Essays on Law and Morality* (Clarendon 1979) 210-229, 212.

[77] See Goldsworthy, 'Legislative sovereignty and the rule of law', 62: 'Arguably, the rule of law is mainly concerned with limiting or controlling what would otherwise be arbitrary power, whether it be exercised by public officials or private citizens. For example, chronic lawless violence inflicted by some citizens on others would surely be as antithetical to the rule of law as the lawless tyranny of a king or emperor.'

including corporations,[78] might figure within the rule of law paradigm are not without merit, but they fall somewhat outside of conventional rule of law understanding.

With these reservations in mind, one can locate the first of the three species of rule of law argument in 'going dark' discourse: encryption threatens rule *by* law, since it enables its users to escape, or operate outside of, the law. This assertion can be tackled from two angles: that rule of (or by) means that the law should be supreme in its power to regulate; and that without properly enforceable law comes anarchy, being the antithesis to rule by law.

4.2.1 Rule by Law as Supremacy of Law

The *supremacy* of law as used herein[79] pertains to the idea that encryption technology reduces the efficacy or relevance of law as a regulatory instrument. This argument parallels decades-old arguments about the ability of law to regulate cyberspace. In this regard, Reed[80] competently summarises the contrasting poles of cyberlibertarianism with cyberpaternalism that have been observed in the development of the nascent internet. Cyberlibertarianism,[81] which denies any role of traditional command-and-control style law to the online realm, is best exemplified by John Perry Barlow's *A Declaration of the Independence of Cyberspace*.[82] Meanwhile, cyberpaternalists argue that national laws do, and should, play a considerable role online,[83] with incisive taglines espoused in academia like *lex informatica*.[84] Arguments on this topic are rarely

---

78 Particularly those with significant regulatory power, as noted by Nijman: 'Behind this legal reality lies the normative reality of the international rule of law ideal: powerful entities that operate to some degree independently on the international plane should be controlled by law and held accountable for their actions.' Janne Nijman, 'Non-State Actors and the International Rule of Law: Revisiting the 'Realist Theory' of International Legal Personality' in Math Noortmann and Cedric Ryngaert (eds), *Non-State Actor Dynamics in International Law: From Law-Takers to Law-Makers* (Ashgate 2010) 91-124, 93.

79 Note that the term often refers instead to the supremacy of laws that constrain governmental action (especially laws with constitutional status): see e.g. Council of Europe Venice Commission, *The Rule of Law Checklist* (European Commission for Democracy Through Law, 2016).

80 Chris Reed, *Making Laws for Cyberspace* (Oxford University Press 2012), Chapter 1.

81 Cyberlibertarianism is defined by Dahlberg as 'the name given to any discourse that sees the Internet and related digital media technology as paving the way to individual liberty, free from centralized bureaucratic systems.' Lincoln Dahlberg, 'Cyberlibertarianism' in George Ritzer (ed), *The Blackwell Encyclopedia of Sociology* (2016) 1-2. See further John Perry Barlow, 'A Declaration of the Independence of Cyberspace' (*Electronic Frontiers Froundation*, 8 February 1996) <https://www.eff.org/cyberspace-independence> [https://perma.cc/Q5MB-XF4G].

82 Barlow, 'A Declaration of the Independence of Cyberspace' <https://www.eff.org/cyberspace-independence>.

83 Reed, *Making Laws for Cyberspace*, 8-9.

84 Joel Reidenberg, 'Lex Informatica: The Formulation of Information Policy Rules through Technology' (1997) 76 Texas Law Review 553. Note also its close etymological relative, *lex cryptographica*, a term which applies to blockchain technologies: see Mimi Zou, 'Code, and Other Laws of Blockchain' (2020) 40 Oxford Journal of Legal Studies 645.

framed in rule of law terms (if at all) however, despite the clear challenges that the online world creates for lawmakers.

Lessig's work on 'code as law'[85] and 'West Coast Code'[86] goes some way in parsing those challenges. On 'West Coast Code', a US-derived metaphor that contrasts the legislative code written in Washington, DC (hence, East Coast Code) with computer code written in Silicon Valley and the like (hence, West Coast Code), Lessig makes the poignant observation:

> West Coast and East Coast Code can get along perfectly when they're not paying much attention to each other. Each, that is, can regulate within its own domain. But the story [changes] "When East Meets West": what happens when East Coast Code recognizes how West Coast Code affects regulability, and when East Coast Code sees how it might interact with West Coast Code to induce it to regulate differently.[87]

The idea that law's relevance is threatened by technological advancement is therefore far from new, and applies to a variety of socio-technical policy challenges beyond encryption. Nevertheless, such occurrences are not typically considered in academic discourse as a threat to the rule of law.[88] Moreover, the proposition that rule of law means rule *by* law, and nothing further, is generally dismissed as being a hollow or even problematic approach by scholars.[89] As put by Tamanaha, 'Rule by law carries scant connotation of legal *limitations* on government, which is the *sine qua non* of the rule of law tradition.'[90]

One might also push back on the idea that encryption, or the providers that offer it, are threats to the supremacy of law in the first place. Those who use or make available so-called 'warrant-proof' encryption are not accused of acting beyond the law as such. At most, the technology companies that offer strong encryption to avoid assisting agencies' investigations might be accused of a form of legal opportunism, comparable to tax *avoidance*, which is lawful, as distinct from tax *evasion*. Framed this way, the argument that agencies are unable to access the plaintext of certain content, despite lawful authority to access it, is in accordance with the design of current law, not in spite of it.[91]

---

85 Lawrence Lessig, *Code: and Other Laws of Cyberspace* (Basic Books 1999).

86 Lawrence Lessig, *Code: Version 2.0* (Basic Books 2006), 72ff.

87 Ibid, 72.

88 Cf. Mireille Hildebrandt and Bert-Jaap Koops, 'The Challenges of Ambient Law and Legal Protection in the Profiling Era' (2010) 73 The Modern Law Review 428, 429.

89 See e.g. Waldron, 'The Rule of Law (Stanford Encyclopedia of Philosophy)' <https://plato.stanford.edu/entries/rule-of-law/#RuleLawRuleLaw>. See also Adam Molnar, Christopher Parsons and Erik Zouave, 'Computer network operations and 'rule-with-law' in Australia' (2017) 6 Internet Policy Review 1.

90 Tamanaha, *On the Rule of Law: History, Politics, Theory*, 34.

91 As put by Raz, '"The rule of law" means literally what it says: the rule of the law. Taken in its broadest sense this means that people should obey the law and be ruled by it.' Raz, 'The Rule of Law and its Virtue', 212.

4.2.2 Rule by Law as Order versus Anarchy

Related to the supremacy of the law is the idea that without the force of law comes anarchy. So-called 'cypherpunks', which are linked to discourse on 'cyber anarchy', perceive unencumbered encryption as central to their version of cyberlibertarianism. As put by proclaimed cypherpunk Timothy May:

> The combination of strong, unbreakable public key cryptography and virtual network communities in cyberspace will produce interesting and profound changes in the nature of economic and social systems. Crypto anarchy is the cyberspatial realization of anarcho-capitalism, transcending national boundaries and freeing individuals to make the economic arrangements they wish to make consensually.[92]

One can make their own conclusions over whether May's 1996 prophecy has since come to fruition. Nevertheless, the above quote at least suggests that encryption can, in principle, act to disrupt normal social order, allowing its users to eschew 'real world' laws and norms.

But is this struggle between order and anarchy an aspect of the rule of law? According to some academics, yes – with Goldsworthy remarking that 'chronic lawless violence inflicted by some citizens on others would surely be as antithetical to the rule of law as the lawless tyranny of a king or emperor.'[93] Belton goes further:

> Law and order is essential to protecting the lives and property of citizens—in fact, it is a prime way of protecting the human rights of the poor and marginalized, who often face the greatest threat from a lack of security. In this end goal, the rule of law is often contrasted with either anarchy or with a form of self-justice in which citizens do not trust in the state to punish wrongdoers and to right wrongs but instead take justice into their own hands and use violence to enforce the social order…
>
> … organized criminals and drug gangs can abuse human rights on just as wide a scale as any government. Thus, high crime rates not only harm law and order, but can also corrupt or overwhelm all rule-of-law institutions and undermine all other rule-of-law ends.[94]

This is similar to the invocations of the rule of law paradigm by Bay and Koops discussed above at 3.2. Belton, however, distinguishes 'law and order' as an aspect of an *ends-based* definition of the rule of law,[95] as opposed to more typical *means-based* definitions. Whilst it is unnecessary to take a position on which approach is preferable, the preponderance of rule of law discourse (which Møller and Skaaning are attempting to systematise in their hierarchy) is means-based, as the latter 'highlight[s] the institutional attributes believed necessary to

---

92 Timothy May, 'Crypto Anarchy and Virtual Communities' (*May*, December 1994) <https://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-virtual-comm.html> [https://perma.cc/8SR8-HWLF].

93 Goldsworthy, 'Legislative sovereignty and the rule of law', 62.

94 Rachel Belton, *Competing Definitions of the Rule of Law: Implications for Practitioners* (Carnegie Papers: Rule of Law Series, 2005), 11-12.

95 Ibid.

actuate the rule of law'.[96] Law and order, therefore, is more typically seen as the other side of the same coin as a means-based rule of law understanding: a society with strong rule of law *means* will organically produce rule of law *ends*, including law and order. Put differently, the most common understandings of the rule of law would not consider encryption's ability to foment a kind of 'cyber anarchy' to be properly framed within the rule of law paradigm.

In any event, one might question whether 'lawless spaces' facilitated by encryption have led to drastic deleterious effects on society's 'order'. Arguably, the negative effects of encryption so far observed are a far cry from the 'chronic lawless violence'[97] or 'organized criminals and drug gangs… abus[ing] human rights on just as wide a scale as any government'[98] given as examples by Goldsworthy and Belton.

4.3 Formal Legality

+ General, public, prospective, certain, equally applied

According to Tamanaha, formal legality means that 'the government can do as it wishes, so long as it is able to pursue those desires in terms consistent with (general, clear, certain, and public) legal rules declared in advance.'[99] Tamanaha notes that formal legality is 'the conception favored by most legal theorists',[100] with Møller and Skaaning adding that the 'notion of formal legality has been hugely influential within the literature'.[101] However, pushing back are scholars critical of formal legality's 'emptiness',[102] with Raz noting as follows:

> A non-democratic legal system, based on the denial of human rights, on extensive poverty, on racial segregation, sexual inequalities, and religious persecution may, in principle, conform to the requirements of the rule of law better than any of the legal systems of the more enlightened Western democracies. This does not mean that it will be better than those Western democracies. It will be an immeasurably worse legal system, but it will excel in one respect: in its conformity to the rule of law.[103]

There are sound reasons, therefore, for opining that the rule of law should be understood as 'thicker' than mere formal legality.

The 'going dark' debate principally intersects with formal legality as it relates to the – often necessary – secretive exercise of power by agencies that deal with

---

96 Ibid.

97 Goldsworthy, 'Legislative sovereignty and the rule of law', 62.

98 Belton, *Competing Definitions of the Rule of Law: Implications for Practitioners*, 11-12.

99 Tamanaha, *On the Rule of Law: History, Politics, Theory*, 96.

100 Ibid, 93.

101 Møller and Skaaning, 'Systematizing Thin and Thick Conceptions of the Rule of Law', 139.

102 Tamanaha, *On the Rule of Law: History, Politics, Theory*, 93.

103 Raz, 'The Rule of Law and its Virtue', 211. Note, however, that Raz does not believe that this conclusion necessarily means that the rule of law is devoid of value.

matters of intelligence and national security.[104] Pro-agency evangelists will find little solace in a formal legality conception of the rule of law.

Relevant, however, to the third of three arguments highlighted earlier at 3.3, the ability of agencies to co-opt private technology companies to assist them is arguably problematic under the formal legality concept. Even before the Snowden revelations, scholars had pointed to the potential for agencies to avoid formal legal channels by engaging the assistance of industry actors to facilitate surveillance. Michaels was one such scholar, who noted in 2008:

> The "War on Terror" has dramatically increased the nation's need for intelligence, and the federal government is increasingly relying, as it does in so many other contexts, on private actors to deliver that information. While private-public collaboration in intelligence gathering is not new, what is novel today – and what drives this inquiry – is that some of these collaborations are orchestrated around handshakes rather than legal formalities, such as search warrants, and may be arranged this way to evade oversight and, at times, to defy the law.[105]

Indeed, one of Snowden's principally noted justifications for his whistleblowing was that he believed that 'the public had a right to know'.[106] One might therefore see technology companies' provision of encryption as one measure to reduce their involvement in such 'handshake' arrangements[107] outside of formal channels of executive scrutiny. In this way, those companies' provision of encryption arguably strengthens the rule of law, rather than weakens it, when seen through a 'formal legality' conception.

4.4 Safeguarded Rule of Law

+ Control (checks + balances)

Møller and Skaaning, describing the third concept in their hierarchy, write that key to 'safeguarded rule of law' is:

> …that the sovereign lawgiver is bound by higher laws, such as those of present-day constitutions, and that an effective separation of powers keeps the sovereign checked… Its institutional manifestation is a system of checks and balances, such as

---

[104] See e.g. Simon Chesterman, 'Secrets and lies: intelligence activities and the rule of law in times of crisis' (2007) 28 Michigan Journal of International Law 553; Atushi Wallace Tashima, 'The War of Terror and the Rule of Law' (2008) 15 Asian American Law Journal 245.

[105] Jon Michaels, 'All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror' (2008) 96 California Law Review 901, 901.

[106] Hubert Seipel, 'Snowden-Interview: Transcript' (*NDR*, 26 January 2014) <https://web.archive.org/web/20140128224400/http://www.ndr.de/ratgeber/netzwelt/snowden277_page-1.html>.

[107] See further Samuel Rascoff, 'Presidential Intelligence' (2016) 129 Harvard Law Review 633, 662ff; Eichensehr, 'Digital Switzerlands'; Rozenshtein, 'Surveillance Intermediaries'.

> an independent judiciary and penalties for misconduct, ensuring that the government/state agents and officials abide by the law.[108]

Much can be carried over from the previous section that discussed rule of law challenges pertaining to matters of intelligence and national security more broadly. Intelligence agencies often operate outside of normal executive limits, with potential rule of law concerns arising from secretive court proceedings, secret courts, or a lack of judicial accountability for agencies.[109] Once again, there is little room for an argument that encryption, or the private entities and individuals that propagate and use it, has a negative impact on intra-governmental checks and balances.

In fact, pointing to concerns (outlined above at 3.3) that pro-agency advocates have about the power wielded by technology companies, a counter argument can be made within this rule of law conception. That is, the ability of these companies, through their provision of encryption, to constrain governments acts as an additional, desirable 'check' on government power.

Michaels,[110] Rascoff,[111] and later Rozenshtein, observe a privatised form of checks and balances. Rozenshtein writes as follows:

> [S]cholars increasingly recognize that to fully understand the separation of powers we must look to factors beyond the internal structure of the government. As Rascoff notes, "The Madisonian insight that individual rights are most effectively protected when '[a]mbition … [is] made to counteract ambition' – a claim that is usually realized through inter- and intragovernmental checks at the federal and state levels" – can be operationalized by the private sector. The private sector's capacity to shape, and even help constitute, the separation of powers is at its height in the domains of technology and communications. And as these domains become ever more central in the twenty-first century, the private sector's influence on our constitutional order will only increase.[112]

In this way, government is limited – and the rule of law *safeguarded* – by the commercial or ideological interests of technology companies. That legal persons can constrain government power is a natural consequence of agency reliance on such actors for surveillance and investigative capabilities. But, as Michaels concedes, the development is not necessarily positive:

> Of course, having private actors serve as government watchdogs in the face of Executive non-compliance is not the most normatively attractive model of separation

---

[108] Møller and Skaaning, 'Systematizing Thin and Thick Conceptions of the Rule of Law', 140.

[109] See e.g. Jack Boeglin and Julius Taranto, 'Stare Decisis and Secret Law: On Precedent and Publication in the Foreign Intelligence Surveillance Court Comment' (2014) 124 Yale Law Journal 2189; Andrew Nolan and Richard II Thompson, *Reform of the Foreign Intelligence Surveillance Courts: Procedural and Operational Changes* (Congressional Research Service, 2019).

[110] Michaels, 'All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror'; Jon Michaels, 'An Enduring, Evolving Separation of Powers' (2015) 115 Columbia Law Review 515.

[111] Rascoff, 'Presidential Intelligence'.

[112] Rozenshtein, 'Surveillance Intermediaries', 108-109, referring to Rascoff, 'Presidential Intelligence', 689.

> of powers, and it may even be seen as excusing (or creating a basis for normalizing) bad behavior by the Executive.[113]

The idea of having to rely on corporations to constrain executive power is particularly concerning given those constraints will occur to the extent that it is in the particular private actor's interests to do so (in most cases, if it is profitable or desirable to shareholders). But, if one perceives the rule of law as pertaining to *constraints* on *government* power, rather than expansions of the same, then technology companies' apparently adverse position towards cooperating with agencies can only be said to *safeguard* the rule of law in this sense.

4.5 Liberal Rule of Law

+ Negative content (liberal rights)

Whereas rule by law, formal legality, and safeguarded rule of law may be regarded as formal conceptions, the latter three conceptions in Møller and Skaaning's hierarchy , starting with liberal rule of law, are best regarded as substantive.[114] The preponderance of rule of law scholarship rejects the inclusion of substantive elements into the rule of law paradigm.[115] Once more, it is not necessary for this paper to take a position on the proper or preferred approach,[116] beyond a further warning that the 'thicker' conceptions discussed hereinafter are to be treated with greater caution than thinner conceptions.

With this proviso made, those advocating thicker, substantive approaches 'call… for augmenting formal legality with individual rights, which are pre-political and constitutionally sanctioned, meaning that they cannot be altered by autocratic rulers or through the democratic channel'.[117] Within these substantive rights, Møller and Skaaning distinguish between so-called 'negative rights' and 'positive rights', finding that:

> According to our reading of the literature on the rule of law, it is … obvious that more agreement exists concerning the inclusion of negative rights into the definition of the rule of law than concerning the inclusion of positive rights; whereas proponents of social rights almost always include negative rights in their definition of rule of law, the opposite is often not the case.[118]

---

[113] Michaels, 'All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror', 965.

[114] There is an argument to be had about whether democracy is a formal or substantive concept; Møller and Skaaning convincingly articulate that 'democracy… is best defined as a set of political rights.' Møller and Skaaning, 'Systematizing Thin and Thick Conceptions of the Rule of Law', 138-139.

[115] Tamanaha, *On the Rule of Law: History, Politics, Theory*, 119; Bingham, 'The Rule of Law', 75ff.

[116] Tamanaha's book spends considerable effort parsing these perspectives: Tamanaha, *On the Rule of Law: History, Politics, Theory*.

[117] Møller and Skaaning, 'Systematizing Thin and Thick Conceptions of the Rule of Law', 141.

[118] Ibid, 141.

The authors do not enunciate what they deem to be negative and positive rights, but they do further specify that negative rights correspond to *liberal* rights, and positive rights correspond to *social* rights. These distinctions broadly correspond with Tamanaha's similar 6-part systematisation of the rule of law, which separates 'individual rights' (including property, contract, privacy, autonomy) from 'social welfare'.[119]

Recall that it was earlier noted encryption has been heralded as a key tool for 'cyberlibertarianism',[120] so far as it – in principle – allows its users to operate free from government interference. Whilst the extent to which cryptography is capable of facilitating a cyberlibertarian utopia of sorts is debatable, it is undeniable that the advent and proliferation of agency-frustrating encryption has bolstered liberal rights in key contexts. The use of encryption by journalists and repressed groups in authoritarian regimes is the eminent example on point.[121] Encryption is a particularly important tool for those whose safety, liberty, or self-actualisation (e.g. through their sexuality, religion, work or activism) may be affected by unobstructed surveillance. In this regard, a recent UN Resolution on the right to privacy in the digital age is illustrative:

> Emphasizing that, in the digital age, technical solutions to secure and to protect the confidentiality of digital communications, including measures for encryption, pseudonymization and anonymity, are important to ensure the enjoyment of human rights, in particular the rights to privacy, to freedom of opinion and expression and to freedom of peaceful assembly and association[122]

Regulatory measures that seek to reduce the availability or efficacy of encryption can likewise be seen as negatively affecting individual liberal rights and hence deleterious to the rule of law in this sense. Moreover, any government attempt to regulate cryptographic speech, such as through *ex ante* design mandates, might similarly be seen as illiberal by constituting an interference on a cryptographer's or tech company's freedom of expression, or a tech company's ability to conduct their business and affairs as they see fit.

That is not to say that cryptography's net positive effect on individual liberty, and regulation's consequent chilling effect on the same, are unimpeachable. The interests – including liberal rights – of victims of encryption-facilitated crime should not be forgotten. Under this concept, the pro-agency side may have a cogent argument that encryption is harmful to liberal rights (of certain groups or individuals). For example, victims of child sexual abuse material and their

---

[119] Tamanaha, *On the Rule of Law: History, Politics, Theory*, 91.

[120] See above at 4.2.

[121] See e.g. David Kaye, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* (2015); Anna Higgins, 'How Strong Encryption Can Protect Survivors of Domestic Violence' (*Internet Society*, 18 December 2020) <https://www.internetsociety.org/blog/2020/12/how-strong-encryption-can-protect-survivors-of-domestic-violence/> [https://perma.cc/SYJ8-YZ39]; Hurwitz, 'Encryption.Congress mod (Apple + CALEA)', 402; Wolfgang Schulz and Joris van Hoboken, *Human Rights and Encryption* (UNESCO Series on Internet Freedom, 2016).

[122] United Nations General Assembly, *Right to privacy in the digital age (A/HRC/48/L9/Rev 1)* (Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development, 2021), 4.

families would likely take little solace that encryption is enabling others' rights to privacy, given it may negatively affect theirs (to say the least) by allowing illegal images to continue circulating online. However, such a right to privacy might better be described as a *positive* right (discussed below), so far as states should be obliged to actively protect individuals' private rights.[123]

4.6 Democratic Rule of Law

+ Consent (lawmakers chosen by competitive elections)

At significant risk of repetition, the 'going dark' debate does not intersect with issues that are at the core of democratic concerns, which relate to the selection of political leaders,[124] and concomitantly the fairness of government elections. Unless the (either inspired[125] or terrible[126]) idea of using encryption-power blockchain technologies for elections is adopted, this is unlikely to change.

Once again, however, the standard framing of the rule of law as applying solely to governmental power can be departed from to facilitate discussion of this concept. At a stretch, democratic rule of law comes in issue when one considers the pro-agency side's third argument: that technology companies exercise significant control over how much investigative assistance they are able to provide agencies. Is the displacement of regulatory power of democratically elected governments towards unelected private organisations, most[127] of which are accountable only to their shareholders, and which have arrived at their position of power purely through the popularity of their products, problematic from a rule of law perspective? The question becomes one of *regulatory legitimacy* – i.e. is the regulatory authority that providers wield in this space *legitimate*?

The conceptual leap from democracy to legitimacy is not a significant one if one unpacks Møller and Skaaning's rationalisation of their fifth rule of law concept, democratic rule of law. This concept adds 'consent', which the authors elaborate to mean 'lawgivers chosen by competitive elections'.[128] Consent relates to what they refer to as the *source* of the rules. For those who adhere to thinner conceptions of the rule of law, the *source* does not matter – what does matter, as put by Møller and Skaaning, is their *shape*. For many legal theorists that see the source of authority as important, democracy is the only *legitimate*

---

[123] Recent European jurisprudence follows this approach: see e.g. *Commission v Hungary (Transparency of associations)*, C-78/18, EU:C:2020:476 para 123; ECtHR, 24 June 2004, *Von Hannover v Germany*, CE:ECHR:2004:0624JUD005932000 para 57.

[124] Brian Tamanaha, 'A Concise Guide to the Rule of Law' (2007) Research Paper Series No. 07-0082 St John's University School of Legal Studies 1, 16.

[125] Jane Susskind, 'Decrypting Democracy: Incentivizing Blockchain Voting Technology for an Improved Election System' (2017) 54 San Diego Law Review 785.

[126] Sunoo Park and others, 'Going from bad to worse: from Internet voting to blockchain voting' (2021) 7 Journal of Cybersecurity 10.1093/cybsec/tyaa025.

[127] Not-for-profits such as Signal and Tor are among those encryption providers without shareholder accountability.

[128] Møller and Skaaning, 'Systematizing Thin and Thick Conceptions of the Rule of Law', 142.

source of power for a government to adhere to a rule of law ideal. As put by Habermas, 'the modern legal order can draw its legitimacy only from the idea of self-determination: citizens should always be able to understand themselves also as authors of the law to which they are subject as addressees.'[129] It is helpful to compare this with non-democratic countries that leverage rule of law terminology, which tend to refer to thinner rule of law concepts,[130] such as rule *by* law, thereby framing the *source* of government power as superfluous to the rule of law paradigm.

The application of 'democratic rule of law' to the actions of non-government entities is evidently problematic, in the form described by Black:

> …non-state regulators in general pose the difficulty that the usual panoply of constitutional mechanisms of accountability which characterize liberal democratic constitutional systems is not necessarily available.[131]

With this in mind, three possible outcomes emerge about the application of Møller and Skaaning's fifth rule of law concept to the 'going dark' debate. First, a nihilistic – though cogent – perspective that providers are doing no more than simply complying with the legal requirements of democratically elected governments, and so their activities do not affect 'democratic rule of law'. Second, that technology companies' role as 'regulators' in the encryption space is troublesome, as they are inherently undemocratic and usurp the regulatory authority of legitimate, democratic governments. And third, that providers actually have a strong claim to regulatory legitimacy in matters relating to 'going dark', and that it is governments themselves that suffer from a deficit of legitimacy.

The regulatory legitimacy of private technology companies has come under increasing scrutiny as they begin to operate in areas of life previously in the public domain and exert influence with a governmental flavour.[132] Concerns abound particularly in areas online, including how they deal with misinformation, disinformation and censorship (e.g. 'deplatforming'[133]); their policies *vis-à-vis* various governments' requests for user information; how they handle user data; the transparency around their internal decision-making;

---

[129] Jürgen Habermas and William Rehg, *Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy* (Faktizität und Geltung Beiträge zur Diskurstheorie des Rechts und des demokratischen Rechtsstaats, MIT Press 1996), 449.

[130] Tamanaha, *On the Rule of Law: History, Politics, Theory*, 112: 'To present just two contemporary examples: China can implement formal legality without democracy, and Iran without human rights, if that is what is desired, with no risk of incoherence.'

[131] Julia Black, 'Constructing and contesting legitimacy and accountability in polycentric regulatory regimes' (2008) 2 Regulation & Governance 137, 140.

[132] Linnet Taylor, 'Public actors without public values: Legitimacy, domination and the regulation of the technology sector' (2021) Philos Technol 1; Nicolas Suzor, Tess Van Geelen and Sarah Myers West, 'Evaluating the legitimacy of platform governance: A review of research and a shared research agenda' (2018) 80 The International Communication Gazette 385; Nicolas Suzor, 'Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms' (2018) 4 Social Media + Society 1.

[133] David Bromell, 'Deplatforming and Democratic Legitimacy', *Regulating Free Speech in a Digital Age* (Springer 2022) 81-109.

cybersecurity more generally,[134] and so on. Evocative titles like iGovernance[135] and 'Digital Switzerlands'[136] succinctly convey the nascent regulatory role of the private technology sector, including that made manifest by the 'going dark' debate. This trend is not restricted to technology, however, with Pariotti noting that, '[d]uring this age of globalisation, the law is characterised by an ever diminishing hierarchical framework, with an increasing role played by non-state actors.'[137]

Indeed, globalism provides a key aspect of providers' claim to legitimacy in matters relating to 'going dark'. Lewis, Zhang and Carter posit that the 'going dark' debate is one of 'global concern, but no global consensus'.[138] Messaging applications operate over a globally connected internet, and smartphones have arguably reached global commodity status.[139] Legal and policy decisions by national governments in the encryption space hence have 'extraterritorial ripple effects'[140] on other jurisdictions, with any regulatory action unable to be restricted to the particular jurisdiction. The conundrum, which is not easily answered, is summarised by Johnson and Post, in their work on borders in cyberspace: '[t]here is no geographically localized set of constituents with a stronger and more legitimate claim to regulate it than any other local group.'[141]

In this vein, it is noteworthy that encryption has also figured on the other side of 'the idea that states should reassert their authority over the internet and protect their citizens and businesses from the manifold challenges to self-determination in the digital sphere.'[142] Following the Snowden revelations, encryption was touted, particularly in Europe, as a potential solution to protect against perceived unlawful or *illegitimate* surveillance by overseas agencies (e.g. the NSA), and

---

134 See Ido Kilovaty, 'Privatized Cybersecurity Law' (2020) 10 UC Irvine Law Review 38.

135 Scott Shackelford and others, 'iGovernance: The Future of Multi-Stakeholder Internet Governance in the Wake of the Apple Encryption Saga' (2017) 42 North Carolina Journal of International Law and Commercial Regulation 883.

136 Eichensehr, 'Digital Switzerlands'.

137 Elena Pariotti, 'International Soft Law, Human Rights and Non-state Actors: Towards the Accountability of Transnational Corporations?' (2009) 10 Human Rights Review 139, 139.

138 Lewis, Zheng and Carter, *The Effect of Encryption on Lawful Access to Communications and Data*, 18. See also Cian Murphy, 'The Crypto-Wars myth: The reality of state access to encrypted communications' (2020) 49 Common Law World Review 245, 258: 'Because of the cross-territorial nature of the phenomenon, unilateral regulation in this field is unlikely to be successful, and yet cooperation remains difficult.'

139 Nicholas Deleon, 'Cellphones now treated as commodity; one-third of people ditch landlines' (*TechCrunch*, 28 April 2008) <https://techcrunch.com/2008/04/28/cellphones-now-treated-as-commodity-one-third-of-people-ditch-landlines/> [https://perma.cc/L5T9-FJN9].

140 Budish, Burkert and Gasser, *Encryption Policy and Its International Impacts: A Framework for Understanding Extraterritorial Ripple Effects.*

141 David Johnson and David Post, 'Law and Borders: The Rise of Law in Cyberspace' (1996) Stanford Law Review 1367, 1375.

142 Julia Pohle and Thorsten Thiel, 'Digital Sovereignty' in Bianca; Herlo and others (eds), *Practicing Sovereignty: Digital Involvement in Times of Crises* (Bielefeld: Transcript Verlag 2021) 47-67, 47-8.

so achieve 'technological sovereignty'.[143] Encryption is therefore a tool that not only challenges domestic states' traditional authority – or perhaps sovereignty[144] – but allows them to curb incursions into the same.

In summation, encryption does not threaten the integrity of democratic processes in the way that most would perceive Møller and Skaaning's fifth concept, 'democratic rule of law'. However, the concept prompts further discussion about the source of rules, and hence regulatory legitimacy, authority, and sovereignty. The following passage from Balkin is apt to describe the state of affairs with regards to legitimacy in the 'going dark' debate: 'Digital information technologies … enmesh individuals, groups, and nations in proliferating networks of power that they neither fully understand nor fully control, and that are controlled by no one in particular.'[145] As Rogaway observes, '[c]ryptography rearranges power';[146] though whether this power rearrangement heralds a positive, negative, or neutral development for a democratic conception of the rule of law is difficult to establish.

4.7 Social Democratic Rule of Law

+ Positive content (social rights)

Møller and Skaaning place 'social democratic rule of law' as the thickest available rule of law concept. This concept adds 'positive rights' to the rule of law, which according to Tamanaha, 'impose… on the government an affirmative duty to help make life better for people, to enhance their existence, including effectuating a measure of distributive justice.'[147] That might include efforts in the provision of healthcare and education services, assistance for the disadvantaged, and so on. To an extent, these measures are uncontroversial – few would argue against the merits of governments facilitating the teaching of children to read, or rolling out vaccines to protect against polio. However, at some point, what was intended by government to be a welcomed intervention to improve social welfare can detract from other rule of law attributes. As put by Tamanaha:

---

[143] Ibid: 'Following reports of foreign government surveillance starting in June 2013, senior officials and public figures in Europe have promoted proposals to achieve "technological sovereignty". This paper provides a comprehensive mapping and impact assessment of these proposals, ranging from technical ones, such as new undersea cables, encryption, and localized data storage, to non-technical ones, such as domestic industry support, international codes of conduct, and data protection laws.' Cf. Tim Maurer and others, *Technological sovereignty: Missing the point?* (2015); Gürses, Kundnani and Van Hoboken, 'Crypto and empire: the contradictions of counter-surveillance advocacy'.

[144] See Ben Buchanan, 'Cryptography and sovereignty' (2016) 58 Survival 95.

[145] Jack Balkin, 'Information Power: The Information Society from an Antihumanist Perspective' in Ramesh Subramanian and Eddan Katz (eds), *The Global Flow of Information* (New York University Press 2011) 232-246, 232.

[146] Phillip Rogaway, *The Moral Character of Cryptographic Work* (Asiacrypt, 2015), 1.

[147] Tamanaha, *On the Rule of Law: History, Politics, Theory*, 113.

> Wonderful as these aspirations are, incorporating them into the notion of the rule throws up severe difficulties. There are already potential conflicts among individual [negative] rights and between rights and democracy; adding social welfare rights to the mix multiplies the potential clashes… The rule of law then serves as a proxy battleground for a dispute about broader social issues, detracting from a fuller consideration of those issues on their own terms, and in the process emptying the rule of law of any distinctive meaning.[148]

Neither Møller and Skaaning nor Tamanaha elaborate significantly on what activities of the state may be done in pursuit of positive rights or social welfare. However, Tamanaha uses the subheading 'substantive equality, welfare, preservation of community'[149] to underlie the sorts of government measures that might fall under this attribute.

Locating such measures in the 'going dark' debate is not straightforward, but one might take aim at the role of agencies as fulfilling a positive right, of sorts. Intelligence and law enforcement agencies all aim to improve the societal conditions in their respective countries, by affirmatively tackling threats to public safety and national security. Against this backdrop, it is arguable that individuals enjoy rights to life, health, privacy, and personal security or safety – and that states have corresponding duties of protection that necessitate law enforcement, intelligence, and military powers.[150] Indeed, European jurisprudence has recognised that 'positive obligations [to respect for private life and freedom from torture or degrading treatment] require, in particular, the adoption of substantive and procedural provisions as well as practical measures enabling effective action to combat crimes against the person'.[151] However, the same courts have been reluctant to recognise a right to security 'as imposing an obligation on public authorities to take specific measures to prevent and punish certain criminal offences.'[152] National security, then, might best be regarded as an 'interest'[153] rather than a positive 'right'. Regardless, so far as there exists a right of individuals to be free from harm facilitated by encryption, these positive rights that contribute to a 'social democratic rule of law' would favour regulatory action, rather than inaction.

---

[148] Ibid, 113.

[149] Ibid, 91.

[150] Liora Lazarus, 'Positive Obligations and Criminal Justice: Duties to Protect or Coerce?' in Lucia Zedner and Julian Roberts (eds), *Principles and Values in Criminal Law and Criminal Justice: Essays in Honour of Andrew Ashworth* (Oxford University Press 2012) 135-155; Christian Starck, 'State duties of protection and fundamental rights' (2000) 3 Potchefstroom Electronic Law Journal 1.

[151] Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature Du Net and Others and French Data Network and Others, and Ordre des Barreaux Francophones et Germanophone and Others* ECLI:EU:C:2020:791 ('*LQDN*'), para 128; referring to *inter alia* ECtHR, 28 October 1998, *Osman v. United Kingdom*, CE:ECHR:1998:1028JUD002345294, paras 115 and 116.

[152] Joined Cases C-511/18, C-512/18 and C-520/18 *LQDN*, para 125 and cases referenced therein.

[153] Daniel Solove and Paul Schwartz, *Information Privacy Law* (3rd ed. edn, Wolters Kluwer 2009), 254: 'Security involves society's interest in protecting its citizens from crimes, including physical and monetary threats.'

Of course, if one accepts that agency activities can be explained by the existence of positive rights, the real conundrum becomes what was forewarned by Tamanaha: that such thick conceptions might tread on the toes of other, thinner rule of law aspects – and other social rights. What is done in the name of national security or public safety, and positive rights thereof, may come at the expense of other positive rights, individual liberty, democracy, or even formal legality.

5 Conclusion

Encryption, users of encryption, and providers of encrypted products and services have been increasingly framed as threats to the rule of law. This paper endeavoured these assertions, which primarily come from government agencies and their supporters for political-rhetorical purposes. The proposition that widespread provision and adoption of (certain forms of) encryption are threats to the rule of law was found to be tenuous – and some might argue disingenuous.

This conclusion is hardly surprising if one takes the orthodox perspective that the rule of law concerns *limits* on government power, not exogenous threats to it. Nevertheless, appreciating the contested nature of the rule of law paradigm, this paper considered a wide range of different available interpretations identified by scholars. Even with a generous approach to what is meant by the 'rule of law', a cogent argument that encryption presents a threat to the rule of law proves difficult to locate, or encounters compelling counter-arguments from the opposing perspective. Regardless of whether one takes a thinner or thicker perspective of the rule of law paradigm, arguing that the net effect of the 'going dark' problem is to detract from the rule of law is at best problematic, and at worst misleading. Advocates of encryption, and rule of law scholars tasked with protecting the paradigm's intellectual integrity, should be prepared to challenge the misuse of rule of law terminology that has become frequent in 'going dark' discourse.

The Performance