UNIVERSITY OF OSLO

Encryption and the Rule of Law

Peter Davis
XXXVI Nordic Conference on Law and Information Technology

9 November 2021

Presentation Aims & Structure

- Broadly outline contemporary ‘going dark’ debate in the ‘West’
  - Jurisdictional focus: USA, EU, Australia
- Outline of ‘rule of law’ invocations in ‘going dark’ discourse
- Parsing of different ‘rule of law’ concepts in literature
- Assessing merits of 3 types of ‘rule of law’ invocations in ‘going dark’ discourse
- Prognosis of ‘rule of law’ paradigm as analytical framework

Snowden: Catalyst for the Contemporary Encryption Debate

- 2013 Snowden revelations
  - Bullrun decryption programme
  - PRISM & participation of tech giants
  - Impact on public trust online & image of tech giants
- 2014
  - Apple & Google announce ‘user-only access encryption’ (UOAE*) by default on mobile OSes
  - WhatsApp announces end-to-end encryption (E2EE) by default
  - Comey ‘going dark’ speech
- 2015 *Apple v FBI* - ‘FBiOS’ case (San Bernardino shooting)
- Since *Apple v FBI* – piecemeal policy & legislative proposals aimed at UOAE & E2EE
  - Broad acceptance of encryption as such; just not ‘warrant-proof’ (hereinafter ‘strong’) encryption
  - Focus on providers (i.e. tech companies)

Accessing Plaintext Despite Strong Encryption: 4 Types of Technical and Regulatory Solutions (1)

1. Use of existing legal and technical capabilities
    - Are we ‘going dark’ or in a ‘golden age of surveillance’? (Swire & Ahmed, 2012)
    - *Apple v FBI* – use of *All Writs Act (1789)*
2. Pure government hacking / lawful hacking
    - Government use of cyber-offensive tools / zero days
    - Use of 3rd party tools (e.g. NSO Group’s Pegasus; Azimuth; Cellebrite)

Accessing Plaintext Despite Strong Encryption: 4 Types of Technical and Regulatory Solutions (2)

3. Encryption design mandates
   - Backdoors, front doors, key escrow, lawful access (?)
     - Ultimate effect – ban of strong encryption
   - Encryption as a content moderation issue
     - Section 230 *Communications Decency Act* amendment? (US)
     - *Digital Services Act* (EU) proposal?
     - Client-side scanning
4. Compelled provider assistance / industry-assisted hacking
   - Australia's *Assistance and Access Act (2018)*

See further Walden (2018); Kuehn & McConnell (2018)

Rule of Law in the ‘Going Dark’ Debate (1)

Virtue signalling or legitimate critique?

- Former Australian PM Malcolm Turnbull, following Hamburg G20 Summit, July 2017:
  - *‘The laws of Australia prevail in Australia, I can assure you of that… The laws of mathematics are very commendable, but the only law that applies in Australia is the law of Australia.’*

Rule of Law in the ‘Going Dark’ Debate (2)

Apple v FBI (US District Court, Central District of California)

- FBI Motion, February 19 2016
  - ‘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’
- Apple Motion to Vacate, February 25 2017
  - ‘[The FBI is] asking this Court to resolve a policy and political issue that is dividing various agencies of the Executive Branch as well as Congress.’
  - ‘…in just such highly-charged and emotional cases that the courts must zealously guard civil liberties and the rule of law and reject government overreaching.’

Rule of Law in the ‘Going Dark’ Debate (3)

Compliance with Court Orders Act of 2016 (US) - Introduced by Senators Burr and Feinstein

- Section 2: It is the sense of Congress that—

  (1) no person or entity is above the law;

  (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’

Rule of Law in the ‘Going Dark’ Debate (4)

EU Council Council Resolution on Encryption, 24 November 2020 –

Security through encryption and security despite encryption

- ‘Protecting 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 to lawfully access relevant data for legitimate, clearly defined purposes in fighting serious and/or organized crimes and terrorism, including in the digital world, and upholding the **rule of law**, are extremely important. Any actions taken have to balance these interests carefully against the principles of necessity, proportionality and subsidiarity.

Rule of Law – to What End?

- Political/PR tool for attaining ‘moral high ground’ in public debate
- Legal doctrine affecting interpretation or legality of (the exercise of) statutory power
- Analytical tool?
  - For evaluating invocations of the ‘rule of law’ in ‘going dark’ discourse
  - Normative framework for assessing merits of regulatory measures?

Rule of Law – Meaning(s)

- Essentially contested concept
- ‘Thin’ and ‘thick’ conceptions
- Systematisations
  - Tamanaha (2004)
  - Møller and Skaaning (2012)

Møller and Skaaning (2012)

Thin

Thick

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)

Tamanaha (2004)

ALTERNATIVE RULE OF LAW FORMULATIONS

Thinner - - - - - - - - - - - - - - - -> to - - - - - - - - - - - - - -> Thicker

FORMAL VERSIONS:	1. **Rule-by-Law** – law as instrument of government action	2. **Formal Legality** – general, prospective, clear, certain	3. **Democracy+ Legality** – consent determines content of law
SUBSTANTIVE VERSIONS:	4. **Individual Rights** – property, contract, privacy, autonomy	5. **Right of Dignity and /or Justice**	6. **Social Welfare** – substantive equality, welfare, preservation of community

Rule of Law and Going Dark

Three primary invocations from law enforcement/intelligence community and their sympathisers

- Encryption as a threat to rule *by* law
  - Circumvent or overcome legitimately enacted law ('lawful access')
- Encryption as deleterious to criminal *justice* and *order*
  - Encryption creating 'safe spaces' for unlawful/immoral conduct
- Technology companies themselves as a threat to the rule of law
  - Using 'technological unilateralism' to stifle surveillance/evidence-gathering and oust democratic law-making
  - *Democratic rule of law* - legitimacy concerns

Encryption and Rule by Law

- Rule by law typically refers to the sovereign (rule by law, not by man)
- Applicability/supremacy of (domestic) law in cyberspace long contested
  - *Lex Informatica* – Reidenberg (1997)
  - *Law and Borders – The Rise of Law in Cyberspace* – Johnson & Post (1996)
- BUT ‘going dark’ debate now focused on centralised providers
  - Digital Wild West or legal opportunism?
- Has law reached its limits? Can law really ‘rule’ in this area?
  - Warrant-proof encryption
  - Regulatory theory and legal sociology – how effective is law as an instrument affecting behavioural change?

Encryption, Criminal Justice and Order

- Criminal justice and rule of law
  - Typically focused on due process (again, rule of law typically applied to governments, not private actors or technologies)
- Law and order as an *end* (not means) of rule of law: Belton (2005)
- How much does strong encryption affect law enforcement/intelligence activities?
  - Going dark vs going spotty / golden age of surveillance
  - Lack of compelling data & lack of trust from national security agencies in matters of cybersecurity/surveillance
- Shifting justifications for anti-encryption measures from terrorism to CSAM

Encryption and Democracy/Legitimacy

- *Apple v FBI*, Government Reply, 10 March 2016
  - 'The rule of law does not repose that power in a single corporation, no matter how successful it has been in selling its products.'
- Tech companies, privacy advocates and strong encryption: a relationship of convenience (& hypocrisy?)
  - 'Digital Constitutionalism'? (Suzor 2018)
  - Platforms + rule of law: is the bigger problem what we *can't* see or what we *can*?
- Cf. Surveillance intermediaries as further 'check' on executive power
  - Government reliance on private networks = power trade-off
  - Rascoff (2016) – 'safeguarded rule of law'

Encryption and Rule by Law – An Alternative to the Security/Privacy Dichotomy?

- ‘Going dark’ debate typically centred around privacy vs security balance, flawed due to:
  - Imprecision of term ‘security’
  - Multiplicity of actors and policy positions – encryption debate no longer binary
  - No account of technical, economic, international etc. challenges
  - No account of power dynamics (tech giants vs domestic agencies)
- Does the ‘rule of law’ paradigm offer a better analytical framework for assessing trade-offs of regulatory (in)action re: encryption?

PhD Thesis: Regulating Cryptography: Rationale and Limits

Prong 1: Internal Limits

- *General Legal Principles & Judicially Enforceable Rights*

- Rule of law as an enforceable legal principle
  - Incl. principle of legality, vagueness, *lex non cogit ad impossibilia*
- *Safeguarded* rule of law - concept inclusive of negative rights (privacy, expression, property etc.)

Prong 2: Systemic Limits

- *Regulatory Theory & Social Systems Theory*

- Rule of law as a rhetorical device: to what extent does/can law actually rule?
- Rule *by* law

Prong 3: Public-Private Limits

- *Regulatory Power of Providers of Strong Encryption*

- Rule of law as a rhetorical device: to what extent does 'big tech' rule?
- Rule of law as including legitimacy (*democratic* rule of law)

Conclusions

- ‘Going Dark’ debate
  - Distinguish ‘going dark’ debate from general encryption problems
- Rule of law and ‘going dark’
  - Mostly virtue signalling; some intellectual merit
- Rule of law generally
  - ‘Congratulatory rhetorical device’ (*Shklar*) or useful analytical tool?
  - Distinguish *legal principle* (e.g. Rechtsstaat) from *political ideal* / conceptions in legal theory
  - In scholarship, critical to stipulate chosen understanding

References

- Kuehn A and McConnell B, *Encryption Policy in Democratic Regimes: Finding Convergent Paths and Balanced Solutions*, 2018
- Møller J and Skaaning S-E, 'Systematizing Thin and Thick Conceptions of the Rule of Law' (2012) 33 The Justice System Journal 136
- Rascoff S, 'Presidential Intelligence' (2016) 129 Harvard Law Review 670
- Suzor N, 'Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms' (2018) 4 Social Media + Society 1
- Swire P and Ahmad K, 'Encryption and Globalization' (2012) 13 Columbia Science and Technology Law Review 416
- Tamanaha B, On the Rule of Law: History, Politics, Theory (Cambridge University Press 2004)
- Walden I, '"The Sky is Falling!' – Responses to the 'Going Dark' problem' (2018) 34 Computer Law & Security Review 1
- Waldron J, 'Is the Rule of Law an Essentially Contested Concept (in Florida)?' (2002) 21 Law and Philosophy 137