A Case for Systemic Design in Criminal Law Techno-Regulation

Brendan Walker-Munro*

The collection and collation of massed data, increasing surveillance, artificial intelligence and machine learning offer huge implications for society. Nowhere is this more evident than in the concept of "techno-regulation", the control of compliant social behaviour by technology. Unlike other scholastic works, this article approaches techno-regulation from a positive position. It suggests that as those charged with the protection of society from its criminal elements, regulators of the criminal law should embrace techno-regulation and squarely confront the risks around its inception. A conceptual model for how a regulator might do so, embedding the precepts of systemic design, is proposed.

INTRODUCTION

Throughout Middle Ages Europe, the concepts of State and Church were inextricably linked in the deployment of the rule of law as a tool of social control. As one of the only mechanisms for controlling society's behaviour, the concept of Christian law was intrinsically interlinked with concept of faith. Mortals who offended the King's peace were subject to the omnipotent gaze and judgment of God.[1] Those convicted of serious crimes were often considered to be *attainted*, a form of "corruption of the blood" where the convict's property was forfeited to the Crown under *civiliter mortuus*. Several centuries later attainder is considered to lie at the roots of modern proceeds of crime legislation which enable seizure of property without conviction.[2] The rise of big data, new digital technologies and the explosion of Internet-enabled devices see something of a return to this omnipotent "gaze from above".[3] Within this turbulent social dynamic, the regulators and enforcers of the criminal law[4] are no less affected by seismic shifts in new technology and changes in normative practice and social conduct.

Whether one considers the scope of regulation of criminal conduct to be "mechanisms of control by the State",[5] establishing standards or rule-setting[6] or as a form of cyclical feedback system between regulated and regulator,[7] the concept of regulation involves the application of pressure (whether it be social, physical or moral) to "change behaviour in order to produce desired outcomes".[8] Yet much of

* PhD Student, Faculty of Business and Law, Swinburne University, Hawthorne, Australia.

[1] Brian Tamanaha, *On the Rule of Law: History, Politics, Theory* (CUP, 2004) 23.

[2] Natalie Skead and Sarah Murray, "The Politics of Proceeds of Crime Legislation" (2015) 38 *UNSW Law Journal* 2, 455.

[3] John Danaher et al, "Algorithmic Governance: Developing a Research Agenda through the Power of Collective Intelligence" (2017) 4 *Big Data & Society* <https://journals.sagepub.com/doi/full/10.1177/2053951717726554>.

[4] For the purpose of this article I consider a **criminal law regulator** to be any organisation or body, empowered or delegated by the State, to regulate provisions of the criminal law, often by investigation and enforcement. This includes police but also (without limitation) food, liquor, safety, transport and environmental regulators.

[5] Philip Selznick, "Focusing Organizational Research on Regulation" in Roger Noll (ed), *Regulatory Policy and the Social Sciences* (University of California Press, 1985).

[6] Julia Black, "What is Regulatory Innovation?" in Julia Black, Martin Lodge and Mark Thatcher (eds), *Regulatory Innovation* (Edward Elgar, 2005); Robert Baldwin, Martin Cave and Martin Lodge, *Understanding Regulation: Theory, Strategy and Practice* (OUP, 2nd ed, 2012) 3.

[7] Christopher Hood, Henry Rothstein and Robert Baldwin, *The Government of Risk: Understanding Risk Regulation Regimes* (Oxford Scholarship Online, 2001); Karen Yeung, "Design for the Value of Regulation" in Jeroen van den Hoven, P Vermaas and Ibo van de Poel (eds), *Handbook of Ethics, Values, and Technological Design* (Springer, 2015) 447–472.

[8] Cary Coglianese, *Measuring Regulatory Performance* (OECD Expert Paper No 1, August 2012).

the literature appears given over to conservative arguments and civil libertarian warnings about the dangers of technology obscuring our freedoms, interfering with our privacy or displacing our humanity. Very little scholarly research appears to focus on the benefits of such technologies, or the argument that regulators ought to "grasp the nettle" on dealing with crime. We therefore intend to develop this counter-argument: rather than adopting the civil libertarian narrative, we instead intend to adopt Tombs suggestion to "engage in radical intellectual work which not only reinstates the possibilities of regulatory options, but recognises that regulation by a capitalist state can only ever deliver a more effectively functioning capitalism".[9]

Before progressing, it is important to acknowledge a limitation in our approach. Our research focuses solely on the State as a pre-eminent source of regulatory power, despite post-modernist views of regulation that have established criminal law regulation is no longer about just "cops, courts and corrections".[10] We take this State-centric view for several reasons. One: even in post-modernism the State as a regulator retains principal interest in ensuring that those subject to potential criminal law treatment are appropriately protected.[11] Two: it is unlikely that the State will ever be wholly divorced from the criminal law process even given the rise of third-party regulation. This is because understanding the unique dynamics of criminal enforcement requires a holistic assessment of the sum of its parts.[12] Three: the State remains uniquely resourced to undertake criminal enforcement.[13] After all, few of the non-State criminal law regulators can match the State for lawful access to information able to ground investigative and compliance outcomes.[14]

We shall therefore propose a positive hypothesis that suggests criminal law regulators can combat disruption by confronting technology (and implementing techno-regulation) more boldly. In Part 1 we will consider disruption and identify that its core element – uncertainty – is what makes disruption so challenging for criminal law regulators. In Part 2 we reflect upon the premise of systemic design as a conceptual framework for criminal law regulators to embed in engaging with the concept of disruption as part of their environments. Part 3 of this article proposes an operational frame around systemic design, and introduces how these concepts might be employed in a systemic design framework.

Part 1: Regulatory Uncertainty in the Face of Disruptors

We live in a world where increasingly "governments use the creation of new criminal laws as the quick fix for social ills ranging from graffiti through drugs to terrorism via dangerous dogs".[15] On reflection, this can be surprising. As elected representatives, Parliaments often demand quantifiable risk to their constituents as justification for proposing or accepting degrees of regulatory intervention, most easily answerable by an answer to the question "where is the harm?".[16] Yet if the target of such laws is rushed, ill-defined, misunderstood, poorly articulated or the regulators' responses are under-resourced, overstated or mired in red tape, society still has a problem.[17] Innovations can become subject to cycles of ill-targeted criminal

[9] Steven Tombs, "Crisis, What Crisis? Regulation and the Academic Orthodoxy" (2015) 54 *Howard Journal of Criminal Justice* 1, 69; see also Kees Dorst, *Frame Innovation: Create New Thinking by Design* (MIT Press, 2015).

[10] John Braithwaite, "The New Regulatory State and the Transformation of Criminology" (2000) 40 *British Journal of Criminology*, 222.

[11] Aaron Fellmeth, "Civil and Criminal Sanctions in the Constitution and Courts" (2005) *Georgetown Law Journal* 94, 98–99; see also Nicola Lacey, "Criminalisation as Regulation: The Role of Criminal Law" (Oxford Legal Studies Research Paper No 50, 2004) 144–167.

[12] Lacey, n 11, 4.

[13] Ian Loader, "Plural Policing and Democratic Governance" (2000) 9 *Social & Legal Studies* 3, 336.

[14] A Mitchell Polinsky and Steven Shavell, "The Economic Theory of Public Enforcement of Law" (2000) 38 *Journal of Economic Literature* 1, 45–76.

[15] Lacey, n 11, 15.

[16] Christopher Hood, *Explaining Economic Policy Reversals* (Open University Press, 1994) 10; Steven P Croley, *Theories of Regulation: Incorporating the Administrative Process* (1998) 98 *Columbia Law Review* 1, 31.

[17] See, eg, our work on Australia's response to encrypted messaging: Brendan Walker-Munro, "A Shot in the Dark: Australia's Proposed Encryption Laws & the 'Disruption Calculus'" [2020] *Adelaide Law Review* forthcoming.

law enforcement as regulators struggle to identify, contain and eliminate risk posed by illegitimate (and sometimes unforeseen) uses of the technology, while ever-new opportunities for illicit enrichment are exploited by an increasingly growing criminal sub-class. In the US literature this disruption is often called "the pacing problem"[18] and "regulatory disconnection" in the United Kingdom and Europe.[19] Though the concept of disruption has roots in the concepts of creative destruction developed by Schumpeter[20] and the disruptive technology of Bower and Christensen,[21] our use of disruption here is intended to be both broader and more inclusive of those original concepts. In other work we engage more heavily with the concept of disruptors and disruption[22] so do not intend to reignite the definitional debate here. Suffice to say for this article, disruptors are an "innovation that disrupt[s] existing regulatory schemes".[23]

Brownsword and Harel describe this as the first and second waves of disruption: the first involving a questioning of the applicability of laws and the second on the content of regulatory responses to disconnection.[24] These waves are observable in the manifestation of what is called the Collingridge dilemma:

> On the one hand, at the early stages of technological development, there is insufficient information regarding potential harms and benefits, but on the other hand, in later stages it can be very difficult, if not impossible, to alter the status quo once the technology has matured, diffusion has taken place and it has become an innovation. In other words, as technological systems acquire momentum and grow larger, and more complex, they also become "more resistant to regulatory prodding". At the same time, the potential implications of many innovations are "not only difficult to predict but are fundamentally unknowable".[25]

It is easy to see that Collingridge's dilemma reflects Brownsword and Harel's two waves of disruption: in the first wave, there is uncertainty about the technology and its reaches and limits. The regulator is cautious and must strike an appropriate balance between the perceived public ills and the promotion of innovation. Their uncertainty limits, constrains or blunts the regulator's response to the emergence of the disruptor in its environment. The second wave occurs, and the regulator has difficulties employing the tools available to it. The disruptor is now more effectively integrated into the society that uses it – including its criminal elements – and the uncertainty instead is around how a regulatory "prod" might be delivered. Yet whatever response could be proposed, we must heed Collingridge's dilemma and ensure that we do not foreclose innovations entirely. The challenge is not an easy one, but the rewards of scholarship in this region are enticing.[26]

Thus, criminal law regulators can influence the emergence of disruption in both a positive and negative way by marking the boundaries of how readily it is incorporated into society.[27] Yet this approaches the

---

[18] Gary Marchant, Ann Meyer and Megan Scanlon, "Integrating Social and Ethical Concerns into Regulatory Decision-making for Emerging Technologies" (2010) 11 *Minnesota Journal of Law, Science & Technology* 1, 345–363; Gary Marchant, Kenneth W Abbott and Braden Allenby (eds), *Innovative Governance Models for Emerging Technologies* (Edward Elgar Publishing, 2013).

[19] Roger Brownsword and Morag Goodwin, *Law and the Technologies of the Twenty-First Century: Text and Materials* (CUP, 2012).

[20] Joseph Schumpeter, *Business Cycles: A Theoretical, Historical, and Statistical Analysis* (McGraw-Hill, 1939).

[21] Joseph L Bower and Clayton M Christensen, "Disruptive Technologies: Catching the Wave" (1995) *Harvard Business Review* 43, 45; Clayton Christensen, *The Innovator's Dilemma* (Harvard Business School Press, 1997).

[22] Brendan Walker-Munro, "Regulating Disruption and the Development of the Disruption Calculus" [2020] *UWA Law Review* forthcoming.

[23] Nathan Cortez, "Regulating Disruptive Innovation" (2014) 29 *Berkeley Technology Law Journal* 175.

[24] Roger Brownsword and Alon Harel, "Law, Liberty and Technology: Criminal Justice in the Context of Smart Machines" (2019) 15 *International Journal of Law in Context*, 107.

[25] David Collingridge, *The Social Control of Technology* (St Martin's Press, 1980), cited in Anna Butenko and Pierre Larouche, *Regulation for Innoativeness or Regulation of Innovation?* (TILEC Discussion Paper DP 2015-007, Tilburg University, March 2015) 16.

[26] Lyria Bennett Moses, "How to Think about Law, Regulation and Technology: Problems with 'Technology' as a Regulatory Target" (2013) 5 *Law, Innovation and Technology* 1, 12.

[27] Roger Brownsword and Han Somsen, "Law, Innovation and Technology: Before We Fast Forward – A Forum for Debate" (2009) 1 *Law, Innovation and Technology* 1, 2.

heart of our problem, as regulators can also suffer disruption. Why then do criminal law regulators suffer from disruption far more readily than civil and administrative counterparts? We suggest that there exists a common theme – that of uncertainty – which not only underscores some of the proposed mechanisms of disruption but also informs a potential response.

Modifying Economic Incentives or "Salience"

The first reason criminal law regulators suffer disconnection more readily is that disruptors can (and often do) modify the economic incentive for crime. The unique structure of the criminal law – which focuses on the traditional duality of punishments by way of fine or imprisonment – means that offenders will generally undertake an illicit act if they anticipate the benefits of doing so will outweigh the anticipated likelihood of being caught and sanctioned.[28] Criminal law regulators thus help define an economic environment by limiting choices, determining transaction costs, and influencing the profitability and feasibility of engaging in certain activities,[29] a proposition that underpins the entirety of the rational choice theory of crime in behavioural economics.[30] This disproportionate market power means a simple regulatory action can result in massive shifts in trading practices and consumer confidence, even if there is a relatively negligible effect on merchant or intermediary costs.[31] Regulators can also influence consumer conduct by shifting their preferences; though this is based on perceptions of availability or affordability, the regulatory conduct can affect either or both (such as by imposition of bans or taxes on regulated goods).[32]

The likelihood of detection, the risk-reward economics of engaging in criminal behaviour, and the perceived deterrent effect of punishment combine to form a variable known as "salience". Salience of law enforcement is a subjective interpretation by a potential offender of the chance that (a) their behaviour will be detected and/or investigated and (b) the likely punishments they could receive for engaging in such behaviour.[33] We hypothesise that the salience of criminal law regulators is a function of the attendant uncertainty of disruption – uncertainty around detection, and/or uncertainty around imposition of punishments. Potential offenders thus engage in the analysis suggested by Lessig: "between [a] norm and the behaviour sought is a human being, mediating whether to conform or not. Lots of times, for lots of laws, the choice is not to conform. Regardless of what the law says, it is an individual who decides whether to conform."[34] It is only logical then that a disruption that causes uncertainty in salience and upsets a regulated populations views about the efficacy, speed, accuracy or timing of a criminal law regulator's approach will result in increased non-compliance.

As an example, the dark web has affected the salience of law enforcement over the past two decades. Traditionally dealings between entities who dealt in illicit commodities such as drugs, firearms, endangered wildlife or contract killings necessitated telephone calls and face-to-face meetings. These

[28] Polinsky and Shavell, n 14, 49.

[29] Douglass North, "Institutions" (1991) 5 *Journal of Economic Perspectives* 1, 97.

[30] Frans Van Winden and Elliott Ash, "On the Behavioral Economics of Crime" (2012) 8 *Review of Law & Economics* 181; Mirko Draca and Stephen Machin, "Crime and Economic Incentives" (2015) *Annual Review of Economics* 7, 389–408; Greg Pogarsky, Sean Patrick Roche and Justin T Pickett, "Offender Decision-making in Criminology: Contributions from Behavioral Economics" (2018) *Annual Review of Criminology* 1, 379–400.

[31] Howard Chang, David S Evans and Daniel D Garcia Swartz, "The Effect of Regulatory Intervention in Two-sided Markets: An Assessment of Interchange-fee Capping in Australia" (2005) 4 *Review of Network Economics* 4.

[32] Quiyan Fan, "Regulatory Factors Influencing Internet Access in Australia and China: A Comparative Analysis" (2005) 29 *Telecommunications Policy* 191.

[33] Gerlinde Fellner, Rupert Sausgruber and Christian Traxler, "Testing Enforcement Strategies in the Field: Threat, Moral Appeal and Social Information" (2013) 11 *Journal of the European Economic Association* 634; Robert Dur and Ben Vollaard, "Salience of Law Enforcement: A Field Experiment" (2019) 93 *Journal of Environmental Economics and Management* 208; compare Alon Harel and Uzi Segal, "Criminal Law and Behavioral Law and Economics: Observations on the Neglected Role of Uncertainty in Deterring Crime" (1999) 1 *American Law and Economics Review* 276.

[34] Lawrence Lessig, "The Zones of Cyberspace" (1996) 48 *Stanford Law Review* 1403, 1408; see also Cynthia Kurtz and David Snowden, "The New Dynamics of Strategy: Sense-making in a Complex-complicated World" (2003) 42 *IBM Systems Journal* 462; Harold Nelson and Eric Stolterman, *The Design Way: Intentional Change in an Unpredictable World* (MIT Press, 2012).

were risky and vulnerable to law enforcement surveillance or undercover operations. Given the prevailing characteristics of the dark web are anonymity and secrecy, it encourages otherwise law-abiding actors to embrace new criminal opportunities. Perhaps unsurprisingly this not only includes supposedly direct forms of criminality (such as selling drugs, firearms or child pornography) but the commission of inchoate offences, such as facilitating others to commit crimes by teaching hacking, child grooming and money or cryptocurrency laundering.[35] Detection of deviance is imperative in criminal regulation – one need only ask the Australian Securities and Investments Commission (ASIC) following their criticism during a recent Royal Commission. By embracing self-regulation of financial institutions with various industry codes, breaches were not adequately detected by ASIC and those that were did not result in deterrent sanctions.[36]

Traditional criminal law regulator responses to disruptions like the darkweb such as crackdowns or targeted enforcement[37] are unlikely to affect the salience of law enforcement because they do not address the underlying paradigm of why the offender engaged in the unlawful conduct in the first place. Because crime is economically rational, a priori criminal offenders are unlikely to react to a perceived increase in policing activity that does not modify their expectations of either detection or punishment.[38] Increased policing activity also does not affect offenders whose offending (though rational) is based on principled resistance or incompetence, because these two forms of response involve "fundamentally different assumptions about their motivations and capacities".[39] Traditional criminal law enforcement responses to disruptors also fail to distinguish between offences that can be contextualised by their conduct; thus, in circumstances of disruption a person who exploits an emerging technology for financial gain is punished the same as one who inadvertently committed an offence through ignorance of the innovation.[40] There are no legal or non-legal grounds to amend or ameliorate the punishment on the basis of the disruptor's emergence.

Nurturing Opportunities for Criminal Entrepreneurship

The second way criminal law regulators are affected by disruption are when markets or processes are created or modified that make offending easier – in effect, their conduct "falls through the cracks" in legal protections.[41] In such volatile markets where new entrants enter or leave at a rapid rate in response to the changing regulatory dynamic, criminality on both small and large scales is rarely far behind.[42] Criminal entrepreneurs are quick to evolve with the times and adapt to the opportunities for financial

[35] Janis Dalins, Campbell Wilson and Mark Carman, "Criminal Motivation on the Dark Web: A Categorisation Model for Law Enforcement" (2018) *Digital Investigation* 24, 69–71.

[36] Commonwealth, Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry, *Final Report* (2019) Vol 1, 105, 315; for a US perspective, see also Joseph A Grundfest, "Future of United States Securities Regulation: An Essay on Regulation in an Age of Technological Uncertainty" (2001) 75 *St John's Law Review* 83.

[37] Daniel Guttentag, "Airbnb: Disruptive Innovation and the Rise of an Informal Tourism Accommodation Sector" (2015) 18 *Current Issues in Tourism* 1192; Michael Gilbert and Nabarun Dasgupta, "Silicon to Syringe: Cryptomarkets and Disruptive Innovation in Opioid Supply Chains" (2017) 46 *International Journal of Drug Policy* 160; Ross Coomber, Leah Moyle and Myesa Knox Mahoney, "Symbolic Policing: Situating Targeted Police Operations/'Crackdowns' on Street-level Drug Markets" (2019) 29 *Policing and Society* 1, 1–17.

[38] Pauline Westerman, "Pyramids and the Value of Generality" (2013) 7 *Regulation & Governance* 80, 80–81; Jonathan Kolieb, "When to Punish, When to Persuade and When to Reward: Strengthening Responsive Regulation with the Regulatory Diamond" (2015) 41 *Monash University Law Review* 136.

[39] Robert Kagan and John Scholz, "The 'Criminology of the Corporation' and Regulatory Enforcement Strategies" in Keith Hawkins and John Thomas (eds), *Enforcing Regulation* (Kluwer Press, 1984) 67–95; Valerie Braithwaite et al, "Regulatory Styles, Motivational Postures and Nursing Home Compliance" (1994) 16 *Law and Policy* 361.

[40] Kevin M Carlsmith, John M Darley and Paul Robinson, "Why Do We Punish? Deterrence and Just Deserts as Motives for Punishment" (2002) 83 *Journal of Personality and Social Psychology* 284.

[41] Brownsword and Goodwin, n 19.

[42] Ken Pease, *Cracking Crime through Design* (Design Council (UK), 2001).

growth that disruptors represent as "disruptive trends … keep perturbing the balance between offenders and preventers".[43]

We would also suggest the idea that some technologies can disrupt criminal law regulation by enabling or lowering the barrier to entry of some form of lawlessness or impropriety quite unrelated to the disruption itself (what some scholars have termed the law of unintended consequences[44]). Gervais describes the law of unintended consequences thus: "No one knew in the 1920s whether airplanes would really be commercially viable for passenger travel, but everyone could picture how they would function if they were. On the other hand, when Michael Faraday invented the electromagnet, no one knew what it would be used for."[45] At this broad level then, the effects of any given technology make for such a difficult regulatory target because for some technologies it is not clear the purposes they could be used for, and for others they are used much as anticipated, but have flow-on social or legal effects that are difficult to anticipate.

Entrepreneurialism for crime can be motivated by regulatory shortcomings, attitudinal responses on the part of regulatees or third-party sources (such as the existence of regulatory havens).[46] As a point of order, it is important to distinguish between the prior section on salience of criminal law regulation versus criminal entrepreneurialism. The former involves failures of the regulator to properly target and effectively telegraph enforcement activities to inform offenders perceptions of detection and punishment. The latter involves motivated or opportunistic non-compliance based on some real or perceived disconnection between the criminal law and its target. Norris and Wilson explain entrepreneurialism thus:

> there will inevitably be those who seek to exploit such [technological] apparatus for less legitimate purposes. The increases in electronic crime, from counterfeit credit cards to terrorists using the internet are an example of how illegal activities are changing in line with the new opportunities this technology creates[47]

Music and film piracy offers an instructive example.[48] Studies have found that income earned by organised crime from media piracy outstrips narcotics trafficking in a number of countries because "profits are huge, the cost of entry minimal, and the risks relatively low".[49] In the Australian market, we were avid consumers and offenders – because of market restrictions on accessing legitimate content Australians were found in a recent study to be some of the most prolific pirates of online movies and TV content.[50] Yet despite the existence of a criminal law framework within which to prosecute such conduct since the early 2000s,[51] no prosecutions of large-scale pirates have been conducted and producers of content for the Australian market increasingly had to rely on civil mechanisms of enforcement.[52]

---

[43] Paul Ekblom, "Technology, Opportunity, Crime and Crime Prevention – Current and Evolutionary Perspectives" in Benoit Lecerc and Ernesto Savona (eds), *Crime Prevention in the 21st Century* (Springer, New York) 336; Philip Brey, "Theorizing Technology and Its Role in Crime and Law Enforcement" in MR McGuire and Thomas Holt (eds), *The Routledge Handbook of Technology, Crime and Justice* (Routledge, 2016) 15–33.

[44] Daniel Gervais, "The Regulation of Inchoate Technologies" (2010) 47 *Houston Law Review* 665; see also William P Marshall, "The Last Best Chance for Campaign Finance Reform" (2000) 94 *Northwestern University Law Review* 335, 342–346; Donald C Langevoort, "The Human Nature of Corporate Boards: Law, Norms, and the Unintended Consequences of Independence and Accountability" (2001) 89 *Georgetown Law Journal* 797, 816–818; Susan Ness, "The Law of Unintended Consequences" (2006) 58 *Federal Communications Law Journal* 531, 532–535; Seth Stoughton, "The Incidental Regulation of Policing" (2014) 98 *Minnesota Law Review* 2179.

[45] Gervais, n 44, 673.

[46] For an excellent summary of these issues, see Brownsword and Goodwin, n 24.

[47] Gareth Norris and Paul Wilson, "Crime Prevention and New Technologies: The Special Case of CCTV" in Duncan Chappell and Paul Wilson (eds), *Issues in Australian Crime and Criminal Justice* (Butterworths, 205) 409.

[48] For background see Bart Cammaerts and Bingchun Meng, *Creative Destruction and Copyright Protection: Regulatory Responses to File-sharing* (LSE Media Policy Project Series, Media Policy Brief 1, Department of Media and Communications, London School of Economics and Political Science, London, UK) 5.

[49] Gregory F Treverton et al, *Film Piracy, Organized Crime, and Terrorism* (Rand Corporation, 2009); Jennifer Hesterman, *The Terrorist-Criminal Nexus. An Alliance of International Drug Cartels, Organized Crime, and Terror Groups* (CRC Press, 2013).

[50] Paula Dootson and Nicolas Suzor, "The Game of Clones and the Australia Tax: Divergent Views about Copyright Business Models and the Willingness of Australian Consumers to Infringe" (2015) 38 *University of New South Wales Law Journal* 206, 224.

[51] *Copyright Act 1968* (Cth) Div 5.

[52] *Roadshow Films Pty Ltd v Telstra Corp Ltd* (2016) 248 FCR 178; [2016] FCA 1503; *Roadshow Films Pty Ltd v Telstra Corp Ltd* (2018) 358 ALR 59; [2018] FCA 582; see also Rajiv K Sinha, Fernando S Machado and Collin Sellman, "Don't Think Twice, It's All Right: Music Piracy and Pricing in a DRM-Free Environment" (2010) 74 *Journal of Marketing* 40.

One might begin to wonder why such matters have fallen by the regulatory wayside and there are several possible reasons, at least demonstrated in the piracy example. The first is that the simple existence of a criminal law is unlikely to engender compliance without the visible taking of some form of enforcement of it,[53] as law is "only one of many types of social regulation such as custom, convention and organized bureaucracies".[54] Another may come from a belief in being a member of a larger group of offenders and "safety in numbers" – again, this differs from the salience of law enforcement by being a considered decision to break the law despite the obvious activities of a criminal law regulator. Perhaps such offenders consider themselves safe in thinking law enforcement have better things to do than chase down small-scale offenders.[55] A third reason involves exploiting the jurisdictional differences between criminal law enforcement, a concept widely regarded as "regulatory arbitrage".[56] The field of regulatory arbitrage is vast (such as differences between international, national, federal, State and local government laws) and may present across as diverse environments as financial services, alcohol sales and illegal waste disposal.[57] While a fulsome discussion of regulatory arbitrage is beyond the scope of this article, I suggest it is enough to reflect that such regulatory arbitrage is fed by the uncertainty caused by disruption. By elevating the likelihood of discrepancies in either legal interpretation or enforcement between multiple jurisdictions, disruption causes uncertainty, and thus increases opportunities for both regulatory arbitrage and criminal entrepreneurialism.[58]

Trust and the Case of the Proper Regulator

The third mechanism by which disruption impacts criminal law regulators arises from traditional understandings of the role they play in society. Police forces especially are rarely the first port of call when a new disruptor makes an impact because the expertise and time required to develop an understanding of a given market and simultaneously deal with the uncertainty of enforcement is not something police forces are generally equipped to deal with, individually or organisationally.[59] Police forces also suffer (as do many regulators) from issues of trust and legitimacy. Increasing community awareness and media scrutiny has eroded popular support for police forces,[60] arguably leaving them less capable of dealing accurately, responsively and appropriately with commercially sensitive decisions in the highly charged social environments enhanced or created by disruption. Within this framework:

> Regulatory state developments not only reform the manner in which public power over economy and society is exercised, but also draw into the process areas of social and economic life in which controls were characterised predominantly as self-regulatory in character[61]

---

[53] Lawrence Lessig, "Law Regulating Code Regulating Law" (2003) 35 *Loyola University Chicago Law Journal* 1, 1.

[54] Hugh Collins, *Regulating Contracts* (OUP, 1999) 6–9.

[55] Mahalia Jackman and Troy Lorde, "Why Buy When We Can Pirate? The Role of Intentions and Willingness to Pay in Predicting Piracy Behavior" (2014) 41 *International Journal of Social Economics* 801.

[56] Victor Fleischer, "Regulatory Arbitrage" (2010) 89 *Texas Law Review* 227.

[57] Jody Freeman and Jim Rossi, "Agency Coordination in Shared Regulatory Space" (2011) 125 *Harvard Law Review* 1131; Alexei Gloukhovtsev, John Schouten and Pekka Mattila, "Toward a General Theory of Regulatory Arbitrage: A Marketing Systems Perspective" (2018) 37 *Journal of Public Policy & Marketing* 142.

[58] For some examples, see Hans Geiger and Oliver Wuensch, "The Fight against Money Laundering: An Economic Analysis of a Cost-benefit Paradoxon" (2007) 10 *Journal of Money Laundering Control* 91. William Simon, "Optimization and Its Discontents in Regulatory Design: Bank Regulation as an Example" (2010) 4 *Regulation & Governance* 3; Gautam Basu, "The Role of Transnational Smuggling Operations in Illicit Supply Chains" (2013) 6 *Journal of Transportation Security* 315; Nicolas Terry, "Regulatory Disruption and Arbitrage in Health-care Data Protection" (2017) 17 *Yale Journal of Health Policy, Law & Ethics* 143.

[59] Janet Ransley and Lorraine Mazerolle, "Policing in an Era of Uncertainty" (2009) 10 *Police Practice and Research* 365.

[60] Adam Crawford, "Policing and Security as 'Club Goods': The New Enclosures?" in Jennifer Wood and Benoit Dupont (eds), *Democracy, Security and the Governance of Society* (CUP, 2006) 111; Kristina Murphy, Lorraine Mazerolle and Sarah Bennett, "Promoting Trust in Police: Findings from a Randomised Experimental Field Trial of Procedural Justice Policing" (2014) 24 *Policing and Society* 405.

[61] Colin Scott, "Regulation in the Age of Governance: The Rise of the Post-regulatory State" in Jacint Jordana and David Levi-Faur (eds), *The Politics of Regulation: Institutions and Regulatory Reforms for the Age of Governance* (Edward Elgar Publishing, 2004).

The advent of Uber in both the US and Australia markets in the late 2000s is a contemporaneous example of this uncertainty. Uber disrupted an existing transport market characterised by static actors (taxis, limousines and charter vehicles) with tightly regulated licensing and pricing controls.[62] This legal framework was not sufficient to capture Uber's service offerings (or was at least ambiguous in its application), but it remained clear that the rationale for legal protection of consumers remained.[63] Authorities in both the United States and Australia suffered from jurisdictional disagreements between local, State and Federal authorities, as well as between police and transport inspectors.[64] The selection of the proper criminal law regulator in times of disruption is tricky enough, but Uber's use of their propriety anti-fraud spyware known as "Greyball" confused the picture even further, believing that the multiple transactions linked to inspectors' credit cards with false names were instances of identity theft.[65]

Flowing from these observations, regulatory arbitrage can also cause difficulties in the selection of the proper regulator. When a disruptor emerges criminal law regulators can struggle to identify who is best placed to provide a regulatory response. It is precisely the uncertainty about who should respond, when they should do it, and how they should respond that results in the disruption of criminal law regulators. We should note that the uncertainty prompted in these situations differs from those regulatory circumstances where the ethics of certain offending behaviour become less stigmatised and thus more difficult to enforce.[66] Such as has been the case with medicinal and recreational cannabis use, where the policy environment has evolved and the legislative strictures around previous criminal activity have been relaxed.[67]

Conclusion to Part 1

In summary then, criminal law regulators face the challenge of uncertainty to retain relevancy and application in circumstances of disruption. With the diffusion of State power and authority through third-party regulators, there are more interpretations and compliance actions taking place in the regulatory space into which a disruptor emerges. Disruption can also decrease the salience of observable law enforcement activity, increase opportunities for criminal entrepreneurialism, or shift the foundations of jurisdiction and legitimacy upon which a criminal law regulator operates. These effects are instructive because they emphasise uncertainty as a key theme to the impact of disruption on criminal law regulators. Uncertainty in decision-making, uncertainty in incentives, and uncertainty in information (also known as information asymmetry) all cause discrepancies, gaps and voids between the various players in regulatory space.[68] So if uncertainty could be the target of a regulatory regime in the face of disruption, how should it be done?

[62] Robert Hardaway, "Taxi and Limousines: The Last Bastion of Economic Regulation" (2000) 21 *Hamline Journal of Public Law and Policy* 319, 331–332; Hannah Posen, "Ridesharing in the Sharing Economy: Should Regulators Impose Uber Regulations on Uber" (2015) 101 *Iowa Law Review* 405.

[63] Christopher Koopman, Matthew Mitchell and Adam Thierer, "The Sharing Economy and Consumer Protection Regulation: The Case for Policy Change" (2014) 8 *Journal of Business, Entrepreneurship & Law* 529.

[64] Brishen Rogers, "The Social Costs of Uber" (2015) 82 *University of Chicago Law Review Dialogue* 85; Igor Dosen and Helen Rosolen, *Uber and Ridesharing* (Department of Parliamentary Services Research Paper No 2, Victoria, October 2016).

[65] Julia Carrie Wong, "Greyball: How Uber Used Secret Software to Dodge the Law", *The Guardian*, 4 March 2017 <https://www.theguardian.com/technology/2017/mar/03/uber-secret-program-greyball-resignation-ed-baker>; Sean Nicholls, Peter Cronau and Mary Fallon, "How Australian Transport Authorities Played Cat and Mouse with Uber's Greyball", *ABC News*, 20 March 2019 <https://www.abc.net.au/news/2019-03-18/how-australian-authorities-played-cat-and-mouse-with-uber/10900892>.

[66] James Moor, "Why We Need Better Ethics for Emerging Technologies" in Jeroen van den Hoven and John Weckert (eds), *Information Technology and Moral Philosophy* (CUP, 2008) 26–39.

[67] Willy Pedersen and Sveinung Sandberg, "The Medicalisation of Revolt: A Sociological Analysis of Medical Cannabis Users" (2013) 35 *Sociology of Health & Illness* 18; Andrew McMillen, "The Snowball and the Avalanche: Medical Cannabis in Australia" (2016) 27 *Matters of Substance* 26.

[68] Butenko and Larouche, n 25, 13; Bennett Moses, n 26, 8.

PART 2: DISRUPTION, UNCERTAINTY AND SYSTEMIC DESIGN

In Part 1 we set out the disruptive waves of change described by Brownsword and Harel. We explored the notion that problems with disruption, disconnection or pacing caused by these waves create areas of uncertainty for the regulator to operate in, altering the compliance spaces and the powers that can (or should) be brought to bear. So, if it could be suggested that responding to regulatory disruption is about responding to uncertainty in some highly complex, open-ended social and political environments, we ought to consider any solution that accepts or incorporates dealing with uncertainty in complex, open-ended systems.

Recent studies have highlighted a burgeoning amount of literature at the interface between the concepts of systems theory and design thinking, collectively referred to as "systemic design". Systemic design leverages the benefits of both concepts: marrying an analytical understanding of the complexities of a target issue with analytically informed, evidence-based and action-oriented responses.[69] Early researches into systemic design have focused on its utility in large-scale environments with interrelated dependent and independent actors including healthcare, urban planning and natural resource allocation.[70] Jones defines typical problems for the application of systemic design as "complex service systems, socially organized, large-scale, multi-organizational, with significant emergent properties, rendering it impossible to make design or management decisions based on sufficient individual knowledge".[71]

Given that this article focuses on the role of regulators (which are complex service systems, socially organised and multi-organisational) in environments of disruption (which have significant emergent properties), systemic design appears to offer significant promise for researchers and practitioners alike. Systemic design also demonstrates significant promise for the criminal law regulators with which this article engages, as existing research supports the adoption of systemic design by State agencies tackling complex problems[72] as well as other regulatory actors.[73] These interactions between the State and citizenry are much characterised by mutable and complex interrelationships between social, political, economic, natural and technology effects (some of which we have already described).[74] Further, as any regulatory environment under disruption involves aspects of "fundamentally unpredictable emergent novelty", as well as systems and organisations that are socially constructed, influenced and reconstructed (which are all hallmarks of a systemic design problem)[75] we would seem well placed to consider systemic design as a potential solution.

In his article on systemic design, Jones describes a four-layered human-centric model for understanding sociotechnical systems: human, work unit, organisation, industry. As one moves into each dimension, the number of actors that it contains and webs of influence between these actors increases both in number and

[69] Peter Jones, "Systemic Design Principles for Complex Social Systems" in Gary Metcalf (ed), *Social Systems and Design* (Springer, 2014) 91.

[70] Michael C Jackson, "Reflections on the Development and Contribution of Critical Systems Thinking and Practice" (2010) *Systems Research and Behavioral Science* 133–139; Peter Jones, *Design for Care: Innovating Healthcare Experience* (Rosenfeld Media, 2013); Sigrun Luras, *Systemic Design in Complex Contexts: An Enquiry through Designing a Ship's Bridge* (PhD Thesis, Oslo School of Architecture and Design, 2016).

[71] Jones, n 69, 94.

[72] Alex Ryan and Mark Leung, "Systemic Design: Two Canadian Case Studies" (2014) 7 *FORMAkademisk* 1; Jonathan Veale, "Systemic Government and the Civil Servant" (2014) 7 *FORMAkademisk* 1; Alex Ryan and Keren Perla, *The Alberta CoLab Experience: Embedding Systemic Design in Government* (Paper presented to Relating Systems Thinking and Design Symposium, Banff, 1–3 September 2015); Uttishta Varanasi, *Life Conservation: A Study into Systemic Design for Wildlife* (Paper presented at Relating Systems Thinking and Design Symposium, Turin, 23–26 October 2018); Terese Bellefontaine and Monica Soliman, *Integrating Systems Design and Behavioral Science to Address a Public Sector Challenge from within* (Paper presented at Relating Systems Thinking and Design Symposium, Turin, 23–26 October 2018).

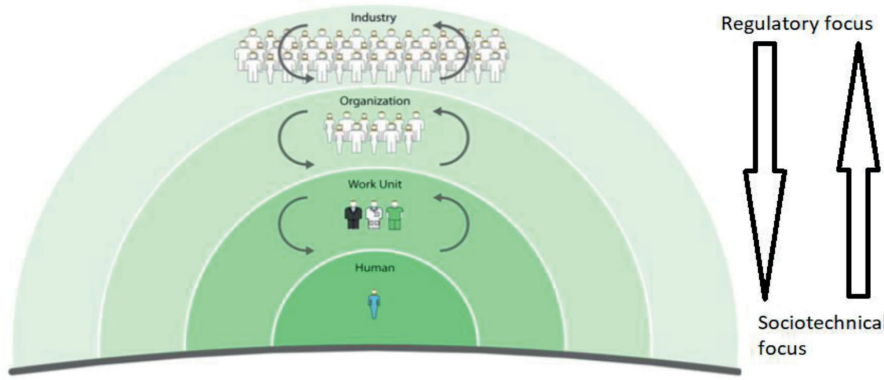
[73] Bridget Malcolm and Mieke van der Bijl-Brouwer, *Developing a Systemic Design Practice to Support an Australian Government Regulatory Agency* (Paper presented at Relating Systems Thinking and Design Symposium, Toronto, 13–15 October 2016); Bridget Malcolm, *Introducing Systemic Design to Support an Australian Government Regulatory Agency Address Complex Problems* (Masters of Design (Research) Thesis, University of Technology Sydney, 2017).

[74] Jones, n 69, 94.

[75] Alex Ryan, "A Framework for Systemic Design" (2014) 7 *FormAkademisk* 10.

complexity. He describes that while the apparent motives of a single human actor may be too difficult to accurately anticipate, nonetheless the human actor "is inserted as a reminder that the purported rationale for the provision of service is to fulfil demands or needs of the given individual. In reality such systems are designed for objectives of the highest-level contexts that supervise the process." What we propose in Figure 1 is an inversion of Jones' model – rather than "bottom up" from individual to industry, we propose a regulator would instead be looking "top down" at the industry it regulates first, and then at the organisations, work units and individuals – how they interact, how they respond, how they move and function within those framesets (and of course, how they commit various crimes within these framesets).

FIGURE 1. Recognition of environment model.[76]



The use of such a model is both supportive and normative when one considers various observations on the future of criminal law enforcement in the literature. First, Jones' descriptions about the degrees of control at each level executed by the individual actors in each space is analogous to control methods that can be encouraged to deter differing crime types, that is robust audit programs for white-collar crime, camera surveillance for property crimes, etc.[77] Second, the model recognises the dense webs of influence prevalent in many different types of crime and the flows in commodity and power between individuals and segments of larger groups.[78] Third, in acknowledging the existence of the human offender within an effectual network of broader organisational and industrial surroundings, the model acknowledges the environmental aspect of criminology that has been lacking in much of the regulatory scholarship to date.[79] Fourth, it accurately represents the "lie of the land" in existing regulatory and security environments.[80] As Fox observed, the key to implementation is the integration of "social requirements of people doing the work with the technical requirements needed to keep the work systems viable with regard to their

[76] Adapted from Jones, n 69, 103.

[77] Mark Andrejevic, "To Preempt a Thief" (2017) *International Journal of Communication* 879.

[78] Jeffrey S McIllwain, "Organized Crime: A Social Network Approach" (1999) 32 *Crime, Law and Social Change* 301; Gail Wannenburg, "Links between Organised Crime and Al-Qaeda" (2003) 10 *South African Journal of International Affairs* 77; Carole Gibbs, Edmund F McGarrell and Mark Axelrod, "Transnational White-collar Crime and Risk: Lessons from the Global Trade in Electronic Waste" (2010) 9 *Criminology & Public Policy* 543.

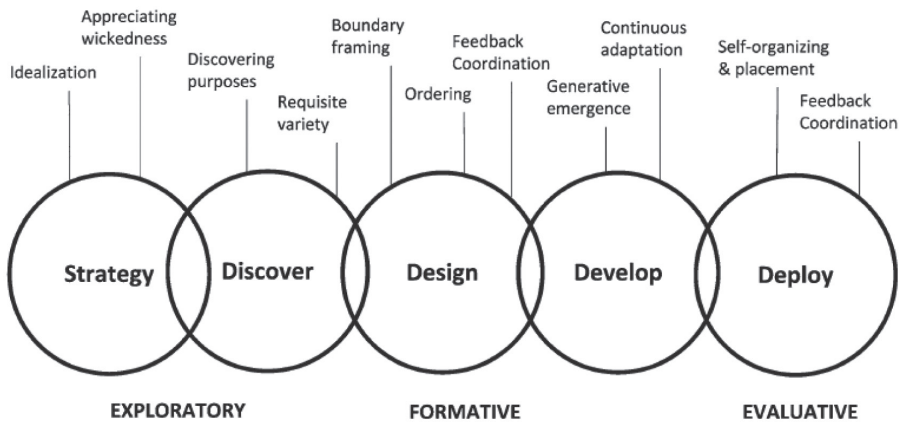
[79] David Weisburd, Cody Telep and Anthony Braga, *The Importance of Place in Policing: Empirical Evidence and Policy Recommendations* (Swedish National Council for Crime Prevention, 2010); Pamela Wilcox and John Eck, "Criminology of the Unpopular: Implications for Policy Aimed at Payday Lending Facilities" (2011) *Criminology & Public Policy* 473; David Weisburd et al, *Displacement of Crime and Diffusion of Crime Control Benefits in Large-scale Geographic Areas* (Campbell Database of Systemic Reviews, Protocol, 2011); John Eck and Emily Eck, "Crime Place and Pollution: Expanding Crime Reduction Options through a Regulatory Approach" (2012) 11 *Criminology & Public Policy* 281.

[80] Malcolm, n 73, 61; Wolfgang Vorraber et al, "UCTM – An Ambidextrous Service Innovation Framework – A Bottom-up Approach to Combine Human- and Technology-centered Service Design" (2019) 7 *Systems* 23.

environments".[81] Unsurprisingly these requirements do not mention legislation or hard-coded rules – a further demonstration that the reaction of increased criminal sanctions to disruption is a distraction of policy and law rather than a substantive solution.[82]

Jones also described 10 shared systemic design principles for complex social systems which have been adopted and promulgated in other studies involving the application of systemic design to complex social systems (though it is worth noting that none of these appear regulatory in nature).[83] These principles are outlined in Figure 2.

FIGURE 2. Systemic design model.[84]



Engaging in building such a systemic design model in Figure 2 requires a number of key changes in existing regulatory thinking as well as practice, in cultivating a focus on *ex ante* prevention rather than ex post cure. At a conceptual level, systemic design cannot properly function without a process of information gathering to better inform idealisation, appreciate the sizes and scales of the "wicked problem" or to help framing of boundaries that are both realistic and achievable. Nor is it possible to inform feedback, self-organise or consider a process of continuous adaptation without gathering information on the interventions being applied and the environment's response to those interventions. This requires a substantial and ongoing investment in understanding the regulated environment. This is not only to determine the layout of the environment as suggested by Jones, but also to inform ongoing feedback and tailoring of interventions once the environment's responses are known. In other work we discuss (by reference to China's social credit system) four key principles that could be adopted by regulators in deploying responses to disrupted environments. Our observations on China's social credit system were deeply informed by the application of the systemic design principles:

- A regulatory focus on individuals or classes of individuals – idealisation, appreciating wickedness, boundary framing;

[81] William Fox, "Sociotechnical System Principles and Guidelines: Past and Present" (1995) *Journal of Applied Behavioral Sciences* 91.

[82] Mark Fenwick, Wulf Kaal and Erik Vermeulen, "Regulation Tomorrow: What Happens When Technology is Faster than Law?" (2016) *American University Business Law Review* 561.

[83] Peter Jones, "Design Research Methods for Systemic Design: Perspectives from Design Education and Practice" (Paper presented at Third Symposium of Relating Systems Thinking and Design, Oslo, 15–17 October 2014); Leah Zaldi, *Building Brave New Worlds: Science Fiction and Transition Design* (Masters of Design thesis, University of Toronto, 2017); Silvia Barbero and Agnese Pallaro, "Systemic Design and Policy Making" (2018) 11 *FormAkademisk* 1; Priscilla Lepre, Leonardo Castillo and Lia Krucken, "Wicked Problems and Design in Emerging Economies: Reflections about the Design of Systemic Approaches Focused on Food and Territory" (2019) *Proceedings of the 3rd LeNS World Distributed Conference* 141.

[84] Jones, n 69, 108.

- Striving for, a system of flawless and contiguous automated surveillance – purposive discovery, appreciating wickedness, continuous feedback and self-orientation in the environment;
- Use of multiple regulatory methodologies to effect changes in behaviour – requisite variety, ordering and continuous adaptation;
- A system of automated response to detect and address risks as or before they arise – purposive discovery, appreciating wickedness, continuous feedback and self-orientation in the environment.[85]

Though most Western democracies would rail against the kinds of systemic controls and draconian authoritarianism exposed in China's treatment of its citizens[86] the importance of this information-gathering is not to be overlooked. The word "surveillance" may conjure up images of uniform-clad security guards watching banks of tiny TV screens, in the modern criminal law environment this analogy is anachronistic. Conceptually, surveillance is no longer limited to mere physical or electronic forms of observation, but rather a system of scrutiny that determines "friend" from "foe" or identifies instances of deviance from some lawful norm.[87]

The benefits of shifting our frame of reference from ex post to *ex ante* are demonstrable in both theoretical and practical contexts. First the mere act of surveillance itself can be a low-cost enforcement tool, as it exerts a powerful disincentive and chilling effect on non-compliance by the regulated population.[88]

Second a purely logical concept is that a crime that is prevented never takes place, and so the loss suffered by the individual or by society is never incurred. For example, when a person has their house robbed, they lodge an insurance claim which will have downstream effects on other policyholders with that insurer. The insurance company will also have a claim to pay out on. The police department will have (generally) one officer's hours to pay for, and there may be additional costs if forensics or property crime taskforces become involved. If the homeowner was uninsured, they suffer financial loss that is never recompensed. Adopting an *ex ante* approach to criminal regulation prevents the crime from occurring and thus forecloses downstream damages.

Third a transition from ex post to *ex ante* enforcement is not as hard as it seems. Since Professor Braithwaite's seminal work on responsive regulation, focus over the last two decades has been on assessing, categorising, sorting and responding to risk. Given that an *ex ante* enforcement environment merely turns to treating risks before they eventuate, much of the hard work already appears done. Zedner makes the analogy work by describing a prison as a "carceral warehouse" of highest risk offenders rather than a tool of punishment or reform.[89]

At a practical level, examples exist of systemic design approaches being taken in regulatory contexts by adopting *ex ante* prevention mechanisms (even when the shared principles themselves are not explicitly called out). Van Brakel and de Hert describe one such instance involving the Dutch Border Control framework where, following a critical report by the Court of Audit of the Netherlands, the border control services committed to a joint information sharing arrangement in which "a comprehensive profile of a passenger and his luggage will be drawn, to assess whether the person needs extra controls".[90] This response required a shared understanding between these various agencies of the "wickedness" of the border control problem, appropriate levels of boundary framing, an employment of requisite variety

[85] Brendan Walker-Munro, "Disruption, Regulatory Theory and China: What Surveillance and Profiling can Teach the Modern Regulator" (2019) 8 *Journal of Governance and Regulation* 23.

[86] Samantha Hoffman, "Programming China: the Communist Party's Autonomic Approach to Managing State Security" (PhD thesis, University of Nottingham, 2017).

[87] Claudia Aradau and Tobias Blanke, "Governing Others: Anomaly and the Algorithmic Subject of Security" (2018) 3 *European Journal of International Security* 1.

[88] Greg Elmer, "Panopticon – Discipline – Control" in Kirstie Ball, Kevin Haggerty and David Lyon (eds), *Routledge Handbook of Surveillance Studies* (Routledge, 2012) 21–29; Nicholas Gane, "The Governmentalities of Neoliberalism: Panopticism, Post-panopticism and Beyond" (2012) 60 *The Sociological Review* 611; Sean Irwin, "Living by Algorithm: Smart Surveillance and the Society of Control" (2015) *Humanities and Technology Review* 28.

[89] Lucia Zedner, "Pre-crime and Post-criminology" (2007) 11 *Theoretical Criminology* 265.

[90] Rosamunde Van Brakel and Paul De Hert, "Policing, Surveillance and Law in a Pre-crime Society: Understanding the Consequences of Technology-based Strategies" (2011) *Technology-led Policing* 175.

of solutions, as well as ongoing feedback coordination, placement of self and adaption to generative problems. Innovations in algorithms in interpreting tax evasion and other economic crimes are another example of the paradigmatic shift to detection rather than prosecution.[91]

Disruption thus requires regulators to combat uncertainty by forcing a shift from ex post mechanisms of respond/investigate/punish to *ex ante* mechanisms of collect/interpret/predict, from crime prosecution to crime control. Though there will probably always be a need for punitive measures as a form of social control and deincentivisation,[92] the rise of technology has given criminal law regulators a new opportunity to respond to criminal conduct either established or encouraged by disruption. As we move into Part 3 of our article, we will turn to consider whether forms of techno-regulation can achieve the heavy lifting for our proposed framework of systemic design.

PART 3: SYSTEMIC DESIGN AND TECHNO-REGULATION

Remembering some of the key propositions from Part 2, a regulatory framework is a complex social service system. It is socially organised, large-scale, complex in nature, and involves substantial interdependence among both vertical and horizontal planes. It is designed to manage, limit or eliminate risk or harm from various spheres of human endeavour or industry. Thus one of the greatest benefits of applying systemic design to a regulatory environment is that it approaches the environment itself as a complex whole, rather than favouring the reductionist paradigms common to much of regulatory practice over the last few decades.[93] The systemic design approach also favours the use of a wide variety of tools (requisite variety), reflecting the cybernetic principle that only variety can destroy variety. Written law, whether in common or statute form, stands little chance against the innovation cycles of tech companies and innovative service providers. Little wonder then that the relative inflexibility of the law has already failed in complex technological domains such as genetically modified organisms, driverless vehicles and artificial intelligence.[94]

But regulators are also, as Brownsword suggests, required to act in a way that is effective, legitimate, and optimally designed. He suggests that technology may, in a form he calls "techno-regulation", design out forms of crime by fixing the environment or fixing the humans that occupy it.[95] There is much attractiveness to such a suggestion. Rather than operating outside the rule of law, techno-regulation can give life and force to it.[96] In addition, as the criminal law regulators with which this article is intended to engage are also organs of the State, techno-regulation offers potential benefits related to speed of reactivity (or even prediction or proactivity), lower transaction costs and efficiency in decision-making – a holy triumvirate for most public agencies.[97] What we hope to achieve in Part 3 is, through the lens of systemic design, to take Brownsword's concept of techno-regulation and extend it into a mechanism for dealing with and proactively responding to disruptions in a regulated environment. Regulators, like those they regulate, must embrace disruption or lose dominance.

---

[91] Geoffrey Warner et al, "Modeling Tax Evasion with Genetic Algorithms" (2015) 16 *Economics of Governance* 165; Lyria Bennett Moses and Janet Chan, "Algorithmic Prediction in Policing: Assumptions, Evaluation, and Accountability" (2018) 28 *Policing and Society* 806.

[92] Joseph Tomain and Sidney Shapiro, "Analyzing Government Regulation" (1997) 49 *Administrative Law Review* 377, 378.

[93] James Giudice, "Through the Lens of Complex Systems Theory: Why Regulators Must Understand the Economy and Society as a Complex System" (2016) 51 *University of Richmond Law Review Online* 101.

[94] Fenwick, Kaal and Vermuelen, n 82, 568.

[95] Roger Brownsword, "What the World Needs Now: Techno-regulation, Human Rights and Human Dignity" in Roger Brownsword (ed), *Global Governance and the Quest for Justice* (Hart Publishing, 2004) 203–234.

[96] Adam Harkens, "The Ghost in the Legal Machine: Algorithmic Governmentality, Economy, and the Practice of Law" (2017) 16 *Journal of Information, Communication and Ethics in Society* 16.

[97] Leighton Andrews, "Public Administration, Public Leadership and the Construction of Public Value in the Age of the Algorithm and 'Big Data'" (2018) *Public Administration* <https://doi.org/10.1111/padm.12534>; see also Michal Gal and Niva Elkin-Koren, "Algorithmic Consumers" (2017) 30 *Harvard Journal of Law & Technology* 311.

As we established in Part 1, most crimes are economically rational; that is, an offender makes a single decision or series of decisions to engage in conduct that is either illegal per se or is preparatory to that act (hence why we have inchoate offences in both common law and statutory forms). Whether it takes the form of false claims on a tax return or insurance form, using company credit cards for personal expenses, or (at its most extreme) planning the serious physical harm or killing of another human being, the offender takes a series of steps designed to bring about their ultimate objective. Thus, criminal law regulators can take as their objective to (a) detect these preliminary steps, and (b) deploy options that defeat them. For many regulators the defeat of offenders is engendered by – in police vernacular, "putting the bracelets on the crook" – the investigation and prosecution of those who commit crimes. It is not until the last decade that criminal law regulators (in common law jurisdictions at least) have considered alternative approaches based on disrupting the economy rationality of offending (such as through proceeds of crime orders[98]).

Only recently have criminological and social theory scholars considered that regulators consider deploying tools that perhaps do not create or actuate punitive disincentives, but rather "dramatise the choice between morality and deviance" to dissuade offenders from engaging in illicit conduct.[99] In effect such tools can be considered "non-law" tools as they do not require an underpinning statutory force to give them life. These non-law tools involve an adaptation of Murray and Scott's "new forms of power"[100] and involve the intersection of four modalities of regulation: hierarchy, community, competition and design:

- **Hierarchy** involves controls borne of systems which includes State law but is not restricted to it, and involve formalistic rules with established sanctions;
- **Competition** involves the self-regulatory effect of market dominance and subservience, that can be harnessed by a regulator in setting conditions of market entry or engagement, or by establishing markets where there are none;
- **Community** is the deployment of controlling behaviour by reference to a societal or group standard, with peer-to-peer and peer-to-superior influence based on societal sanctions involving shame or ostracisation;
- **Design** of regulatory tools that, by their very nature, foreclose non-compliance or provide regulatory oversight in a way that a regulatee cannot influence (such as the way a taxation authority selects for audit).

By way of demonstration, consider the following: a burglar has robbed a bank and makes off with several thousand dollars. This conduct is illegal and most countries have laws established that makes bank robberies illegal – yet this does not stop them occurring. However, the technologies now deployed in many banks and financial institutions (24-hour delay safes, high-resolution surveillance cameras and UV-marked bills) involve an order of magnitude more sophistication to circumvent, meaning offenders must be more willing to risk their freedom to commit robberies. Some of these tools are outlined in Figure 3 and discussed in our work on Australia's recent encryption laws; such as delegating regulatory power to the marketplace, so that only compliant actors can access markets to sell their goods and services, implementing physically engineered technological countermeasures, or cultivation of social stigma with certain kinds of unwanted conduct, such as that associated with bankruptcy or "name and shame" orders.

[98] Skead and Murray, n 2, 455.

[99] Karen Yeung, "Towards an Understanding of Regulation by Design" in Roger Brownsword and Karen Yeung (eds), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Hart Publishing, 2008) 98.

[100] In turn modelled from Lawrence Lessig's work on "code": Andrew Murray and Colin Scott, "Controlling the New Media: Hybrid Responses to New Forms of Power" (2002) 65 *The Modern Law Review* 491.

FIGURE 3. Opportunities for techno-regulatory (non-law) responses.[101]

Surveillance technologies likewise form part of the techno-regulatory framework. For example, the law – inherently a hierarchical control – may allow a police officer with a court order (such as a search warrant) to enter a person's home and search it for evidence of a crime. However, a suitably robust surveillance network would observe that person committing the offence at first instance, which may be enough to prevent the offence from occurring in the first place – in this respect the surveillance system has operated as a design element, as it has foreclosed the offending conduct (the person chooses not to offend on the basis they know they will get caught!). Lawrence Lessig is oft-cited when he said "Code is an efficient means of regulation … There is no choice about whether to yield to the demand for a password; one complies if one wants to enter the system. In the well implemented system, there is no civil disobedience."[102] Enforcement in this example has become perfected.[103]

As is evident from the preceding examples, the dissuasive effect of techno-regulation can be achieved by setting barriers that either foreclose non-compliance completely, make it more obvious when such non-compliance is engaged in, or make it easier to be detected. However, it is important to observe that the shift from ex post to *ex ante* conduct contemplated by both techno-regulation and systemic design involves a consideration of how mens rea will be interpreted in attributing criminality.[104] In quoting Marx,

[101] Walker-Munro, n 17.

[102] Lawrence Lessig, "The Zones of Cyberspace" (1996) 48 *Stanford Law Review* 1408.

[103] Karen Yeung, "Can We Employ Design-based Regulation While Avoiding *Brave New World*?" (2011) 3 *Law, Innovation and Technology* 6.

[104] Ian Leader-Elliott, "Framing Preparatory Inchoate Offences in the Criminal Code: The Identity Crime Debacle" (2011) 35 *Criminal Law Journal* 80.

Samuel Nunn explained the transition of the new technologies as shifting from reasonable suspicion of a single suspect to a categorical suspicion of everyone.[105] This poses a series of challenges to the human rights of "everyone", who may or may not be involved in preparing for, facilitating or committing a given crime. From a popularist viewpoint, these concerns are articulated in the movie *Jurassic Park* by the fictional character Dr Ian Malcolm who, when confronted with the idea of cloning dinosaurs from DNA fragments in fossilised insects, proclaims that "your scientists were so preoccupied with whether or not they could, they didn't stop to think if they should".[106]

The bundle of human rights principally associated with techno-regulation (involving protections of privacy, independent agency and a right to due process) is colloquially referred to as the "right to be left alone". Curiously this collection of rights is not as novel as it appears. In 1890, Warren and Brandeis described human rights such as these as under attack from "[i]nstantaneous photographs and newspaper enterprise … numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops'".[107] A century later in 1991, Booth argued that true security comes from emancipation, not from order foisted on the citizenry by the executive.[108] In 2014, Ashworth and Zedner describe that the requirements of a *ex ante* criminal system promotes intervention before reasonable suspicion and thus "stands in acute tension with any idealized account of a principled and parsimonious liberal criminal law".[109] It is important thus to consider now how human rights might not be inconsistent with a properly systemically designed, techno-regulatory framework. Beyleveld and Brownsword helpfully describe what they see as being the important principles in treating criminal conduct from a techno-regulatory standpoint – relevance, accuracy, proportionality, least restrictiveness, precaution and just compensation[110] – and so we shall adopt these for a more fulsome exploration of our systemic design framework.

Relevance, at least in the terms argued by Beyleveld and Brownsword, is ensuring that the targets of techno-regulation are crimes that sufficiently offend the concepts of good citizenry. Yet relevance is a concept difficult to square with at least one broader concept in the criminal law, particularly the State's duty to criminalise certain conduct. Regulatory offences may reference "rules and penalties for their breach",[111] yet the legislature must still have identified some ethical or moral wrong sitting as the root cause for that offence. For example, companies that do not file their tax returns by the due date or erect safety scaffolding for its workers may infringe regulatory offences, but this does not mean the conduct satisfying those offences is any less blameworthy or attracting in criticism. Here we would adopt Harel's conclusion that the State has a duty to criminalise and enforce those breaches, not only in protection of the rights of innocent citizens but also in public declaration that those rights are important to the State.[112]

Relevance also becomes less applicable if we pair techno-regulation with a "human in the centre". If we recall Jones' environmental model, we remember that a human actor resides in the centre. Given the nature of current predictive technologies is only to highlight areas of greater risk and help guide the deployment of resources,[113] there is still plenty of opportunity for regulatory agents to determine what those resources are, how they react and what they do when they examine at that person or place.

[105] Samuel Nunn, "Seeking Tools for the War on Terror: A Critical Assessment of Emerging Technologies in Law Enforcement" (2003) 26 *Policing: An International Journal of Police Strategies & Management* 454.

[106] *Jurassic Park* (Universal Studios, 1993).

[107] Samuel Warren and Louis Brandeis, "The Right to Privacy" (1890) 4 *Harvard Law Review* 193.

[108] Ken Booth, "Security and Emancipation" (1991) 17 *Review of International Studies* 313.

[109] Andrew Ashworth and Lucia Zender, *Preventive Justice* (OUP, 2014) 251.

[110] Deryck Beyleveld and Roger Brownsword, "Punitive and Preventive Justice in an Era of Profiling, Smart Prediction and Practical Preclusion: Three Key Questions" (2019) *International Journal of Law in Context* 198.

[111] Antony Duff, "Perversions and Subversions of Criminal Law" in Antony Duff et al, (eds), *The Boundaries of the Criminal Law* (OUP, 2010) 88–112.

[112] Alon Harel, "The Duty to Criminalise" (2015) 34 *Law and Philosophy* 1.

[113] Orla Lynskey, "Criminal Justice Profiling and EU Data Protection Law: Precarious Protection from Predictive Policing" (2019) 15 *International Journal of Law in Context* 162.

Techno-regulation that contains a human circuit breaker is therefore far more likely to be trusted, legitimised and accepted.[114]

Accuracy refers to the idea that, for a techno-regulatory system to be considered legitimate and effective, it must be capable of "applying penal sanctions to agents who have committed an offence".[115] There is rhetorical force in the argument, as false positives or false negatives by their very nature erode trust and legitimacy of the process and techno-regulation in general, and waste regulatory resources.[116] Take bag screening at an airport. We accept the necessity of such checks in our lives because of the collective security that it offers knowing that all of our fellow passengers have been checked for weapons, drugs and explosives. However, if the screening technology broke down often, or subjected more than the reasonable share to invasive bag searches or let through a terrorist with a bomb in his luggage, we would be far less trusting and accepting of the technological fix. Yet this perhaps unnecessarily narrows the true scope of techno-regulatory accuracy, which we submit instead lies in properly selecting *prospective* lawbreakers from compliant citizens – a true positive – or inversely, selecting compliant citizens from *prospective* lawbreakers – a true negative. Though Brownsword may argue that techno-regulation "collapses the distinction between is and ought"[117] the terms used here are more than just euphemisms. Returning to our bag screening example, the X-ray is merely an indicator of risk – current generation scanners do not automatically decide that "that shape is a weapon" and subject the bag's holder to arrest and detention. Instead, it flags the bag for further inspection by a trained Customs officer who makes subsequent decisions regarding criminal liability (if any). Thus the inherent attraction in panopticon-style surveillance and techno-regulation is not necessarily in the concept that enforcement might be perfected, but that it is better than using human eyes and human decisions.[118] Beyond that, techno-regulation is about incentivising compliant behaviour rather than de-incentivising illicit behaviour (though it may also have this effect, as bag scanners probably already discourage would-be terrorists and drug runners from using commercial air flight).

Proportionality, at least in the terms adopted in the literature, describes that particular penal sanctions should be proportionate to the crime being treated. This would seem to make thematic sense – deploying a 24-hour, CCTV surveillance and ambient law enforcement algorithm to automatically fine jaywalkers who do not cross at a defined crossing point would seem to be an overly paternalistic, borderline draconian response to a relatively minor form of offending. However, there are two problems with this approach: first, we are using our techno-regulatory framework to simply "enable" existing enforcement tools (ie fines); and second, we are not considering a true techno-regulatory approach where the offender might be estopped from jaywalking in the first place. Public order offences such as this might hypothetically respond more positively to community methodologies of control, such as widespread citizen surveillance (using mobile phones to transmit evidence directly to the regulator) combined with advertising designed to shame offenders.[119] The question about proportionality instead becomes one about ensuring that the regulated environment has at least some degree of trust in the deployment of the tool, rather than in the fact that the deployment is done automatically. Take for example Twitter's three strikes policy. Though instances of serious malfeasance, stalking or predatory behaviour are dealt with immediately, one-off breaches of community standards results in suspensions and strikes, where three strikes results in account termination. Appeals can be made against both account termination and the imposition of strikes.[120] Instances of "three strikes" policies in legal contexts are rare but not unheard of,

[114] Mireille Hildebrandt, "Law as Computation in the Era of Artificial Legal Intelligence: Speaking Law to the Power of Statistics" (2018) 68 *University of Toronto Law Journal* Suppl 12.

[115] Beyleveld and Brownsword, n 110, 206.

[116] Ronald Leenes, "Framing Techno-Regulation: An Exploration of State and Non-State Regulation by Technology" (2011) 5 *Legisprudence* 143.

[117] Roger Brownsword, *Law, Technology, and Society – Re-imagining the Regulatory Environment* (Routledge, 2019).

[118] Bennett Moses and Chan, n 91.

[119] See, eg, the NSW Environmental Protection Agency's "Don't be a Tosser!" Campaign: EPA <https://www.epa.nsw.gov.au/your-environment/litter-and-illegal-dumping/epa-work-prevent-litter/dont-be-a-tosser>.

[120] Stuart Macdonald, Sara Giro Correia and Amy-Louise Watkin, "Regulating Terrorist Content on Social Media: Automation and the Rule of Law" (2019) 15 *International Journal of Law in Context* 192.

such as the disciplinary provisions in the *Liquor Act 2007* (NSW) where the imposition of strikes, though administrative in character, are also subject to judicial scrutiny and review.[121]

The principle of least restrictiveness argues that criminal sanctions should only be used to the extent that it is necessary. Later in their article, Beyleveld and Brownsword discuss the example of Rosa Parks who engaged in civil disobedience by sitting in the "Whites Only" section of her bus. They argue that her conduct drew attention to the plight of African Americans of the time, but occurred only because the transport system was inefficient and under a techno-regulatory system, may never have occurred at all.[122] While the arguments for least restrictiveness are couched in terms of allowing civil disobedience to contribute to active citizenship, this Precaution argues that appropriate safeguards ought to be included in techno-regulation to ensure redress is available for the innocent. An intriguing debate on this topic occurred between Hans Somsen and Luigi Corrias in 2011 which particularly focused on this aspect of techno-regulation. In commenting on the debate, Lemcke stipulated that where both Somsen and Corrias appeared to agree was that the potentially paternalistic controls of a techno-regulatory system could be ameliorated by proper ombudsman and monitoring by a citizenry.[123] Ombudsmen at both State and Federal levels have wide discretionary powers to inquire into aspects of public administration and make clear what the basis for controls is and how this affects the actions of the citizenry. In circumstances where a techno-regulatory approach has been taken, perhaps the idea of an algorithmic ombudsman is not so distanced from the ideal solution.[124]

Finally, just compensation is not a foreign concept to criminal regulation, nor even to forms of techno-regulation. Indeed, it was from the types of concerns that Warren and Brandeis agitated for in the 1890s from which arose the legal concept of a tort for injurious falsehood, modification of the doctrines of libel and slander (now defamation in most jurisdictions) and imposition of statutory instruments relating to privacy at the international and State levels. The General Data Protection Regulation in the European Union, championed as one of the high watermarks in global privacy law, is not prima facie inconsistent with the idea of predictive policing, profiling or "generalised suspicion".[125] In addition, both the Independent Reviewer of Terrorism Legislation[126] and the House of Lords[127] have found existing privacy and legal protections were not inconsistent with the widespread surveillance and intrusion powers of many UK investigative agencies. Thus, one could feasibly argue that the importance here is not on determining a scale of whether compensation is "just" (which can be undertaken under existing legal strictures) but on distinguishing whether compensation is available in the first place. In many cases the original decision will not be overturned unless such fresh evidence is presented that the verdict is unsafe or it would run counter to public policy to allow a conviction to stand.[128] The law will endure – decisions made under a techno-regulatory scheme by a computer are still "decisions" capable of judicial interpretation, scrutiny and (if necessary) censure.[129]

Thus, a properly considered, systemically designed techno-regulatory framework that considers (but may not always use) non-law tools is one well placed to resist the effects of disruption. This invites the

[121] Julia Quilter, "Sydney's Lockout Laws: Cutting Crime or Civil Liberties?" (2016) 28 *Current Issues in Criminal Justice* 93.

[122] Beyleveld and Brownsword, n 110, 214.

[123] Oliver Lembcke, "Techno-regulation and Law: Rule, Exception or State of Exception? A Comment to Han Somsen and Luigi Corrias" (2011) *Netherlands Journal of Legal Philosophy* 2.

[124] Nicholas Diakopoulos, "Algorithmic Accountability Reporting: On the Investigation of Black Boxes" (Briefing Paper, Tow Center for Digital Journalism, 2014) <https://academiccommons.columbia.edu/doi/10.7916/D8TT536K/download>.

[125] Lynskey, n 113.

[126] David Anderson QC, *Report of the Bulk Powers Review* (Report presented to Parliament by Command of her Majesty, August 2016).

[127] House of Lords, *Surveillance: Citizens and the State* (Select Committee on the Constitution, 2nd Report of Session, 6 February 2009).

[128] *R (on the Applications of Hallam and Nealon) v The Secretary of State for Justice* [2016] EWCA Civ 355; compare *R (Adams) v Secretary of State for Justice* [2011] UKSC 18.

[129] See, eg, *Pintarich v Federal Commissioner of Taxation* (2018) 262 FCR 41; [2018] FCAFC 79.

consideration of future research in the area, where perhaps we might close our article by suggesting one such line of enquiry. In their article, Wright and De Filippi argue for the rise in the *lex cryptographia*, a unique strand of law comprised of self-executing smart contracts. Such smart contracts would link to the Internet of Things, public and private sector databases to inform themselves as to whether the contract's conditions precedent have been fulfilled. If they have not, the contract executes changes or modifications to system accesses for the parties to the contract, limiting or eliminating their ability to pursue further repudiatory conduct. From our regulatory standpoint, a person might be given access codes to their car under a self-executing smart contract with the State. If they exceed the speed limit too often, or run too many red lights, the smart contract changes their access to the car and estops future criminal conduct. Such a techno-regulatory scheme may seem a whimsical notion, but in effect the law here continues to act as a hierarchical control – it simply takes a different form to what it does now.

CONCLUSION

Like the metamorphosis of medieval attainder into modern proceeds of crime orders, the all-knowing and omnipotent God of the medieval church has been given new life in the form of State techno-regulation. By harnessing the concepts of big data, analytics and artificial intelligence to generate insights from massed datasets, agencies of the State can predict the behaviour of regulated environments and deploy regulatory "nudges" with greater and greater accuracy. We argue that the marriage of these two fields offers an exciting area of research that can be deployed to assist regulators to predict and respond to a wide variety of crime types, irrespective of the displacing effects of technology. Not only do the effects of disruptive technologies become less important, we argue this approach offers a chance to fuel the regulator's move from a highly reactive and slow-moving leviathan to a nimbler agency operating in concert with a more secure "pre-crime" society. This said, when designing such a system, regulators need to remain keenly aware of their obligations to citizens' rights to protections of privacy, independent agency and a right to due process.