Regulating Disruption: Blockchain, GDPR, and Questions of Data Sovereignty

JOURNAL OF INTERNET LAW
VOLUME 22
NUMBER 2
AUGUST 2018
EDITED BY DLA PIPER

Regulating Disruption: Blockchain, GDPR, and Questions of Data Sovereignty

By Robert Herian

A REGULATORY CONUNDRUM

In *The Regulatory Enterprise*, Tony Prosser proposes two regulatory visions at once in dialogue and polar opposition, as well as acknowledging a degree of hybridity constituting regulatory environments and spaces of control, something which influential voices in technology regulation, namely Lawrence Lessig, have been accused of underplaying in order to assert the argument 'that there is considerable novelty to the nature of law in Cyberspace'[1]. There is a 'major distinction', claims Prosser, 'between regulation as infringement of private autonomy and regulation as a collaborative enterprise', and this, I suggest, is applicable to the blockchain regulatory conundrum[2]. For present purposes, the former, an emphasis on autonomy, can be said to accord with a vision of blockchain put forward by the ecosystem

Continued on page 8

Dr Robert Herian *is a Lecturer in Law at The Open University, UK. His teaching and research interests include private law, technology regulation, economic and political philosophy, critical theory and psychoanalysis. This essay is adapted from: Robert Herian,* Regulating Blockchain: Critical Perspectives in Law and Technology. *London: Routledge (forthcoming 2018)*

Wolters Kluwer

The Control by and Rights from page 1

based on neoliberal market-complementing regulation, economic efficiency, and self-interest, and what Prosser further refers to as "regulation for economic efficiency and consumer choice."[3]

In his discussion of liberty and trust within a (neo) liberal moral and legal framework, Joseph Raz defines autonomy or the "capacity for valuable autonomous life" as a "double-side duty" (or what might otherwise be deemed a deliberate contradiction) requiring "government to stand back and let people have the choice as to how to conduct their own lives," but equally government taking "active steps, where needed, to ensure that people enjoy the basic capacities (physical and mental) and have the resources to avail themselves of an adequate range of options available in their society."[4] On the other hand, the latter, regulation as a collaborative enterprise, enables political, social, or distributive feasibility, community, and generosity, or what Prosser aligns to "regulation for social solidarity" and "regulation as deliberation."[5] A fourth regulatory framework highlight by Prosser concerns the protection of rights[6]; regulation rooted in domestic and trans-national legislative frameworks, as well as international law and treaties, which do not necessarily favour either the polarity of markets and self-interest or community and generosity unless predisposed to do so by law.

Cutting across each of the positivist regulatory frameworks, however, is a natural law tradition and a potential for equity that aims at mollifying the harder edges of the regulatory enterprise and arguably underscoring the deliberative conditions that Prosser touches on. It is here that we can locate "the good" in relation to blockchain, although it is important, not least given regulatory uncertainty that is central to the blockchain regulatory conundrum, to understand the role the good plays when applied to the regulation of blockchain, rather than simply notions of the good free-flowing from the blockchain ecosystem as a product of particular techno-economic concepts and use-cases—a notion of the good that arguably accords with "an empty space into which human choice may move."[7] Notions of the good drawn from *inter alia* Plato, Aristotle, and Hobbes are instructive here, as is, with particular regard to Prosser's fourth regulatory framework, translation of the good as a moral determination of justice to a regime of enforceable (contractual) rights. In the background, however, it is important to remember the problems created by attempting to pin-down the good. As Iris Murdoch maintains, the concept of the good "remains obscure and mysterious," and we all "see the world in the light of the Good, but what," she asks, "is the Good itself?"[8]

Although Plato and Aristotle rejected the good as rooted in subjectivism, both maintain the import of human nature in defining what goods are or ought to be. For Plato the role of human nature "is not to define or set the good, but merely to define what the possibilities of human achievement are."[9] Similarly, Aristotle holds that, "what makes it true that something is good is not that it stands in some relation to desire but rather that it is somehow *perfective* or *completing* of a being, where what is perfective of completing of a being depends on the being's nature."[10] In contrast, Hobbes forefronts desire in determinations of the good, and it is this form that arguably best describes regulatory processes such as self-regulation. Subjectivist theories of the good makes true what is good as that which is desired or liked, and thus the good for Hobbes always returns to notions of self-preservation which manifest clearly in, for example, efforts to forestall legislation that restricts the global investment practices of technology titans like Google, and lead them instead to enter into self-regulation pacts in order to retain control within the limits of self-interest.[11]

Also, brief mention of the shift from good to right is important here because it is fundamentally a continuation of an enlightenment colonization of economic rationality over all social life, whereby contract is the ultimate arbiter of human interrelatedness negating the need for honesty or trust to flourish outside of contractual domains and agreements. Conditions, moreover, which are further reinforced by a suite of contractual remedies that insist on performance as well as compensation and damages. Equity as body of law, in this sense, arguably preserves contractual domains while countermanding the resilience of non-contractual social relations and status. The importance of contract in the blockchain context cannot be overstated, not least because of the importance placed on the burgeoning field of so-called smart contracts (as well as "secret contracts") as a new and potentially global modern contractual regime-in-waiting. Smart contracts are certainly not capable of supplanting

contract law as we presently find it, but the hope of many stakeholders is that it soon will.

Melanie Swan, for instance, addresses the matter via a typical problem/solution matrix. "Contracts do not make anything possible that was previously impossible," she claims, "rather, they allow common problems to be solved in a way that minimizes the need for trust. Minimal trust often makes things more convenient by taking human judgement out of the equation, thus allowing complete automation."[12] For Swan, therefore, the journey from an ethics rooted in human discretion (morality, equity, natural law, and so on), to enlightenment social rationalisation in the form of contract is *perfected* by blockchain, to recall the Aristotelian notion of the good, and the opportunity for full automation of contractual agreements and the rendering *autonomous* of all forms of human interrelatedness over which contract has long principally held sway. And recalling Hobbes, Swan also suggests that "smart contracts impact not just contract law, but more broadly the notion of the social contract within society."[13]

It is important to note that what Swan and others in the blockchain ecosystem are proposing is not so much radical due to novelty—contract long ago shifted the texture of social interactions and as an offline and off-chain technology has been supremely successful, perhaps more so than blockchain and smart contracts are ever likely to be. Instead, radicalism is to be found in the apparent attempt within the blockchain ecosystem to forge a linkage between a metaphysic of "the good" and the instrumental performativity inherent to contractual status. Moreover, that this connection should be made by machines and software *automatically* and *autonomously* rather than as a precondition of human needs, rights and desires, thus skewing and intertwining the logic of "the good" and contract. "A technological innovation may know long periods of stagnation or regression," Félix Guattari argues, "but there are few cases in which it does not 'restart' at a later date."[14] The suggestion here is not that the technology or mode of legal technique of contract has not been anything but alarmingly present throughout modernity. What has amounted and continues to amount to the good, in comparison, is more contentious. Yet smart contracts may well indicate a *restart* of contract and especially in the performativity of *contracting*, as implied by Guattari, through (re)alignment with 'the good', although the consequences of this remain unknown and potentially hard to determine.

The current task of understanding what *regulating blockchain* means or ought to mean is occurring against a backdrop of continuing struggles to achieve stable regulation and governance of commercial platforms, within networks, and in consideration of interoperability and the broader architecture of the Internet. Few, it might be said, would argue that Internet regulations have succeeded in producing universally held "good" behaviour or conduct. The questions, problems, and so on that blockchain brings to the fore are not easily abstracted from concerns that continue to plague regulation of Internet-based networks and systems, and from the perspective of capital these concerns often coagulate around perceived and actual systemic inefficiencies that technologies bring to bear.

There is a phylogenetic evolution of network technologies, in which blockchain can be included, exposed to formal and informal (customary) standards and benchmarks for improving efficiency gains in business (and beyond), with any subsequent determinations of effectiveness those technologies herald linked directly and primarily to net gains in economic efficiency. This emphasis on efficiency is arguably a product of neoliberalism generally, although Michael Power attributes it more specifically to the audit culture that has matured during the last 40 years of neoliberalism. "At the level of these technologies," claims Power, "practitioners constantly debate the efficiency of different methods and seek to elaborate cost-efficient solutions to the problem of providing assurance."[15] "Accordingly," he concludes "even audit techniques are surrounded by sub-programmes and meta-discourses about their potential. *Technical practice cannot be disentangled form the stories which are told of its capability and possibility*" [emphasis added].[16]

Further, as Brownsword argues: "one of the facts of regulatory life is that there is no easy way out of deep moral disagreement. It is a problem that has taxed moral and political philosophers; and it is a problem that will continue to plague the regulation of new technologies."[17] Shortcomings in Internet regulation remain stubbornly apparent some 30 years into the mass adoption of the technology.[18] The how's and why's of blockchain regulation now form part of, but have also arguably intensified, the broader regulatory conundrum started by the Internet. There are a number of reasons for this claim. Of most interest here,

however, is one that concerns the co-evolution of technology and economy and, importantly, associated cultural and political ramifications, and how regulatory environments, enterprise and rationale address them. If, for example, it is true that the "economy is an expression of its technologies," it is equally so, I claim, that technologies are the expression of economic will, and the present blockchain moment is both illustrative *and* symptomatic of the latter, rather than the former.[19]

DISRUPTING REGULATION

The emergence of so-called blockchain "disruption" within the contemporary political and economic moment calls to mind Joseph Schumpeter's notion of *creative destruction*.[20] In the hands of quasi-libertarian, self-interested and what Vinay Gupta has called, "chaotic" entrepreneurs, this creative destruction has led, in the main, to myriad attempts at re-imagining (*not* disrupting) legacy financial systems over the last decade using cryptocurrencies within the scope of capitalism.[21] The desire now is to repeat the process in an array of noncurrency based, normatively civic arenas such as e-voting, land registries, and health records.[22] In practice, this means growth in blockchain-based private-public partnerships, or to put it another way an upsurge in tendering for *privatization* of forms of public administration that will put many more future data controllers beyond direct political accountability (private corporate actors not being publicly elected officials).

So-called blockchain 2.0 and 3.0 projects are thus following a model of evolving capital-led projects: from those of a classical liberal economic age in which capital was front and centre in all modes of business, commerce and industry, to the more ambiguous and obscure role capital now plays in the strategies of misdirection and sleights of hand of neoliberalism. Amid shifts in economic/regulatory models the role of regulators has been amplified by the perverse matrix of behaviours and attitudes these technologies have created and continue to create. Regulation is, however, also being denied, resisted, and sent into retreat based on the idea that centralized government authorities and regulators are ill-equipped and ill-prepared for the task of dealing with technology or high levels of chaos and white-noise emanating from the blockchain ecosystem.

The so-called wait and see or the somewhat more proactive 'wait and monitor" approaches to regulation adopted by the likes of the European Commission are symptomatic not of a reasonable approach to blockchain, but, I argue, of an unwillingness by governments to muster the energy, let alone the resources, to challenge private self-interest.[23] "Drawing up regulations for blockchain at this early stage would be a mistake," argued *The Economist* in 2015, "the history of peer-to-peer technology suggests that it is likely to be several years before the technology's full potential becomes clear. In the meantime regulators should stay their hands, or find ways to accommodate new approaches within existing frameworks, rather than risk stifling a fast-evolving idea with overly prescriptive rules."[24] Narratives of regulatory weakness such as the one presented by *The Economist* and disseminated by technology ecosystems like that of blockchain are being accepted by governments and regulators as fundamental truths. Further, practices of rhetoric and persuasion have enabled competition and markets to intercede and translate regulatory frameworks and techniques in their own image. Standardization, for example, whilst considered *contra* the interests of devotees of free markets who "characterize regulation as simply an unnecessary cost to business," is nevertheless only good at the end of the day for delivering economies of scale that will be of benefit to ever larger markets.[25]

Again there is nothing new about any of this. What is happening around blockchain is merely a continuation of regulatory trends that have remained constant for at least 40 years, accept, perhaps, during the collapse of public confidence wrought by the 2008 financial crisis which forced governments to change tack from fewer to more (apparent) regulations.[26] In the context of technology, the change in regulatory bias notably occurred within financial services and created the outgrowth of FinTech (financial technologies) and RegTech (regulatory technologies), respectively. However, this resulted in greater commitments by governments to innovationist narratives and working with a reserve army of entrepreneurs prepared to play in "sandboxes." This sandbox culture as the *sine qua non* of contemporary regulatory standoffishness at the state level has ultimately spawned the problematic regulatory conundrum with which we are now faced, one in which innovationism and solutionism have been legitimized.

Attempts by entrepreneurs to leverage personal, self-interested gains through the re-imaging of various legacy systems, are occurring at the fuzzy edges of transnational regulatory understanding and leading to the threat of regulatory disorientation, whereby focus is stuck on "centralized actors in a decentralized ecosystem" and, therefore, "will not be able to keep pace."[27] Jurisdictions have as a consequence reacted at different speeds, some slow, others with more urgency, especially in the case of cryptocurrency regulation, which has included in some cases outright bans on the trading and possibly also on the use of cryptocurrency.[28] Nevertheless, as yet the majority of jurisdictions have said little and done less to define or impose limits on blockchain specifically, nor on its ecosystem or the conduct produced by it. This "wait and see" approach, it would appear, is a longer term project, a fact that is only welcome if that means serious critical scrutiny of the technology is undertaken in the meantime.[29]

Where it is problem, however, is twofold: firstly, where the wait and see policy is beholden to forms of innovationism or creates a vacuum that innovationism quickly fills; something often made clear by calls from entrepreneurs and other stakeholders for government not to stifle innovation[30]; secondly, in allowing a lag between law, regulation, and governance and blockchain to grow in the interim. Both problems, which largely intersect, repeat the shortcomings and mistakes of Internet regulation which have led to the explicit dominance of big data business and the mass commercialization of cyberspace on the one hand, and a parallel ungovernable 'dark-net' on the other hand. Whether the problem is seen as central (legitimate and notionally legal big data business) or peripheral (dark web as shadow or black markets), there is a clear shared dialogue between the innovative capabilities of the technologies in use.

Ironically, if we follow Ilkka Tuomi's definition of innovation as relating to technologies that lead to tangible change in social practices, it is more likely than not that the peripheral uses innovate first and further.[31] Milton Mueller reinforces this point, whilst also simultaneously celebrating innovation and highlighting failures in Internet regulation and governance. "It has become a cliché," says Mueller, "to note that the 'unified and unfragmented space' created by the victory of the Internet protocols was filled not only with *innovative economic and social activity*, but also with the crimes and conflicts that accompany human interactions in every other space" [emphasis added].[32] Thus, Mueller concludes, "[a]long with the innovations, efficiencies, and creative new forms of entertainment and interaction came thieves, bullies, fraudsters, child abusers, spies, vandals."[33]

Although blockchain may not be considered a particularly risky technology in terms of potential threats or harms, it poses to individuals or communities—compare this with, for example, cautionary tales surrounding "the malign aspect of technology" that includes perceived threats from bioengineering, artificial intelligence, and nanotechnologies—this does not mean that *no* threats or harms exist. Instead, these manifest in other, more subtle ways.[34] There are, for instance, conceivable threats and harms posed by the blockchain ecosystem in further entrenching and disseminating neoliberal ideology. For neoliberal stakeholders and those complaisant about the ill-effects of social and political control wrought by "free-market" economics, this is unlikely to sound like a threat at all. For this class of stakeholder blockchain remains, for the better, "an institutional technology to decentralize the governance structures used to coordinate people and economic decision making."[35] If, however, neoliberal ideology is grounded in what Stuart Hall called the anachronism of "the free, possessive individual, with state cast as tyrannical and oppressive," whereby the state "must not intervene in the 'natural' mechanisms of the free market, or take as its objective the amelioration of free-market capitalism's propensity to create inequality," then what is at stake in the regulatory decisions that foster or mitigate *more* neoliberalism in the blockchain context ought to be clear, questioned and ultimately challenged, because they *do* represent threats and the potential for harm.[36] G.A. Cohen is less forgiving than Hall in the language he chooses to criticise markets, but the conclusions the two reach are nevertheless in accord:

> The immediate motive to productive activity in a market society is typically some mixture of greed and fear, in proportions that vary with the details of a person's market position and personal character. In greed, other people are seen as possible sources of enrichment, and in fear they are seen as threats. These are horrible ways of seeing other people, however much we have become habituated and inured

> to them, as a result of centuries of capitalist development.[37]

Cohen is robust in his critique of free-market ideology, and although he also deals at length with the more germane issue of regulation in his criticism of John Rawls, it is his "antimarket" discourse that provides a vocabulary for tackling the blockchain regulatory conundrum as it is understood here, and in particular to feed the double meaning of *disrupting regulation*, as the ability of regulation to disrupt, as well as be disrupted. It offers, therefore, a principled basis for thinking about blockchain regulation not from the point of view of neoliberal free-market ideology, a position Cohen claims is motivated by "greed and fear," but from commitments to "fellow human beings and with a desire to serve them while being served by them."[38] Cohen continues:

> I mean, here, by 'community', the antimarket principle according to which I serve you not because of what I can get out of doing so but because you need my service. That is antimarket because the market motivates productive contribution not on the basis of commitment to one's fellow human beings and a desire to serve them while being served *by* them, but on the basis of impersonal cash reward […] The genius of the market is that it recruits shabby motives to desirable ends, and, in a balanced view, both sides of that proposition must be kept in focus. Generosity *and* self-interest exist in everyone. We know how to make an economic system work on the basis of self-interest. We do not know how to make it work on the basis of generosity. But that does not mean that we should forget generosity: we should still confine the sway of self-interest as much as we can.[39]

Cohen's call "to confine the sway of self-interest" resonates closely with the regulatory enterprise required in the blockchain context, but also more generally as well. Finally, regulating blockchain as it is defined here asks whether blockchain is a necessary technology in a given context versus alternative technologies or even, perhaps, whether the option of no technology at all is or might be the most appropriate response. This approach asks the question of why nobody has found a use for blockchain in the 10 years of its existence.[40] Moreover, it echoes a pragmatic turn by the United States Bureau of the Fiscal Service (BFS) toward evaluations of blockchain use and relevance in a given context. For example, on the BFS website under the heading "Determine if Blockchain is a Good fit" is the following framework:

> To help you determine if blockchain is a potential solution, you can apply criteria to your use case. If you answer "yes" to several of these questions, a blockchain solution may be worth considering:

- Do you need a structured central repository of information?
- Is more than one entity reading or writing transactions to a database?
- Is there less than total trust between parties/entities in the ecosystem? (for example, one user will not accept the "truth" as reported by another user)
- Are central gatekeepers introducing costs and /or "friction" when verifying transactions (for example, manual verification)?
- Are there routine or logical interactions that occur that could be programmed to self-execute (for example, smart contracts)?[41]

GDPR VS BLOCKCHAIN

A notable manifestation of the blockchain regulatory conundrum involves the General Data Protection Regulation (GDPR) introduced by the European Union (EU) in May 2018 to replace the 1995 Data Protection Directive. The regulation represents an extraordinary and, in some cases, unwelcome new reality in the blockchain ecosystem as a continuation of the European Union's "particularly strong constitutional tradition of privacy protection" and development of EU data protection law.[42] What is more, GDPR actually performs a number of functions that data sovereignty models on blockchain perform, most notably in terms of giving back control of personal data to data subjects, thereby arguably undermining many blockchain business models.[43]

The EU's influence in this regard extends far beyond the boundaries of the Union, which thus implies a far-reaching impact of the GDPR for blockchain use-cases that do not specifically, intentionally, or directly involve personal data of EU citizens. "The EU has successfully influenced other regional privacy laws by restricting the transfer of personal data from member states to countries without adequate privacy protection," Brown and Marsden point out, and this "determination of 'adequacy' overseen by the European Commission, in practice requires other states to introduce most of the key protections [from EU data protection directives and regulations] into their own national laws."[44]

It is important, albeit briefly, to note GDPR here even though potential impacts remain speculative at the time of writing, because the regulation is likely to affect a wide range of blockchain use-cases in the EU and beyond. Key questions for the GDPR versus blockchain debate begin with the matter of control of personal data, specifically who within the context of a blockchain application is controlling data and thus accountable for its administration within the scope of the regulation. As Jacek Czarnecki maintains: "The controller determines the purposes and means of the processing of personal data. Does such an entity exist at all in the context of a distributed blockchain? We can potentially treat transaction-confirming miners as controllers (in the case of the proof-of-work consensus)—something that in the case of large public blockchains will be unfeasible in practice."[45] Control equally concerns jurisdiction, in terms of the jurisdiction in which a data controlling party (blockchain node or miner for example) is located and thus the possible or extent of the laws governing them. Winston Maxwell and John Salmon also point to the impact upon issues of control wrought by the different varieties of blockchain, namely permissioned, permissionless, and so on.[46]

The impact of the GDPR on use-cases flowing from the blockchain ecosystem is certainly not negligible, and impact assessments will likely be necessary for use-cases relating to permissionless, public blockchains, as well as those for civic service management of sensitive data such as health records.[47] The necessity of impact assessments for private or enterprise blockchain is less clear however, as Andries Van Humbeeck maintains: "An important aspect of GDPR on blockchain is the fact that personal data is not to leave the EU. This is a major problem with public blockchains, since there is no control on who hosts a node. This is less an issue when it comes to private or permissioned blockchains."[48] In this sense, the GDPR is arguably already performing a broad-ranging *ex ante* regulatory function that some blockchain stakeholders will view as counterproductive to innovation.

Rights for "data subjects" under GDPR include: access to personal data and supplementary information, which involves submission of a subject access request (SAR); objections to certain forms of processing including direct marketing and for research and statistics; rectification of inaccurate and incomplete personal data; erasure of personal data, otherwise known as "the right to be forgotten"; the restriction of processing of personal data; rights relating to profiling and automated decision-making, a right that could impinge upon the "invisible" machine-to-machine capabilities that blockchain is able to facilitate via smart contracts; and claims for compensation for damage caused by a data breach. Further, limitations on transferring data and information outside of the European Union other than for prescribed reasons, places restrictions on the free-flow across geographical and jurisdictional space. Many of the rights and restrictions the GDPR introduces contradict the ways in which existing global computer network operate, and this includes blockchain.

Of the new rights, the right to be forgotten (Art. 17) is one which does not sit comfortably with what for many stakeholders are core and desirable features of blockchain, namely the ability of "immutability" to create "transparency" in order to foster "trust." It is important to note that "erasure" is not an absolute right to be forgotten under the terms of the legislation however, and if, for example, the data involve defence of a legal claim or have overriding public interest, then a data controller can refuse to comply with the right. "The goal of GPDR is to 'give citizens back the control of their personal data, whilst imposing strict rules on those hosting and 'processing' this data, anywhere in the world," says Van Humbeeck, and "one of the things GDPR states is that data 'should be erasable.' Since throwing away your encryption keys is not the same as 'erasure of data', GDPR prohibits us from storing personal data on a blockchain level. Thereby losing the ability to enhance control of your own personal data."[49] For Van Humbeeck, this is the paradox

of GDPR and blockchain. Maxwell and Salmon describe the issue further:

> One of the design features of blockchain architecture is that transaction records cannot be changed or deleted after-the-fact. A subsequent transaction can always annul the first transaction, but the first transaction will remain in the chain. The GDPR recognises a right to erasure. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. What constitutes "erasure" is still open to debate. Some data protection authorities have found that irreversible encryption constitutes erasure. In a blockchain environment, erasure is technically impossible because the system is designed to prevent it.[50]

The right to be forgotten linked to the erasure of personal data thus strike at the heart of the immutability of blockchain. Following the logic above, once immutability is brought into question or falls completely through general implementation of mechanisms for undoing chains, this brings into question both the creation of transparency and the ability to foster trust. And, some will argue, without the ability to foster trust or at least to do so without the evil necessity of having to rely on institutional middlemen like banks or government, what is the point of blockchain?

For use-cases to remain viable an industry in workarounds that exploit cracks in the detail of the GDPR have been in business since the reality of what GDPR would entail began to emerge in the blockchain ecosystem in early 2017. "Smart contracts will contain mechanisms governing access rights," claim Maxwell and Salmon, "therefore the smart contract can be used to revoke all access rights, thereby making the content invisible to others, albeit not erased."[51] Meanwhile, "a popular option to get around this problem is a very simple one," says Van Humbeeck, "you store the personal data off-chain and store the reference to this data, along with a hash of this data and other metadata (like claims and permissions about this data), on the blockchain."[52] On the other hand, as Van Humbeeck also admits, the term "workaround" is a clear acknowledgement of the regrettable positon the GDPR puts the ecosystem in, and that "compromise is rarely good for business."[53] This is an illustration of the point that classic regulatory conundrums turn on the extent to which regulatees are compliant or can made to be compliant in the future. As Stuart Biegel maintained with regard to the Internet but in terms arguably appropriate for the present discussion:

> Under current conditions, given the highly participatory nature of online activity and the distributed, anarchic design of cyberspace itself, there are a host of ways to get around most restrictions that may be imposed. In addition, new architectural changes can often be countered by other code-based solutions. Thus a proposed regulatory approach may not be possible unless those that have the ability to resist agree to go along with the plan.[54]

At the time of writing the ramifications of the GDPR versus blockchain debate remain inconclusive. What is obvious already, however, is a desire for blockchain stakeholders to exploit, as best they can, uncertainties existing within the four corners of the GDPR using *know-how* or as Biegel suggests "the ability to resist." Thus while the regulation is forcing compliance to some extent, it is by no means watertight and concerns for regulators ought to surround greater desires to undermine the regulations rather than comply with them. Test cases in the coming months and years will be necessary for the further interpretation of the regulation and these are guaranteed to emerge as stakeholders push blockchain concepts and use-cases to the limits of compliance. Quite what "compliance" means in terms of blockchain is, of course, itself yet to be meaningfully or authoritatively defined by regulators or the wider legal community.

NOTES

1. Tony Prosser, *The Regulatory Enterprise* (Oxford University Press, 2010) 4; Andrew Murray & Colin Scott, "Controlling the New Media: Hybrid Responses to New Forms of Power", 65(4) *The Modern Law Review*. 504 (2002).
2. Prosser, *Supra* n.1 at 4. The distinction is made more apparent when the nature of different blockchains is taken into consideration. Namely, *permissioned ledgers*, which, as the name suggests, are designed for use on closed, private systems by those with the requisite permissions (*e.g.*, to create a "transparent" and "immutable" information and data audit trails *within* the confines

of a global corporation); in contrast to permission-less ledgers like the Bitcoin blockchain which maintain a public character and are therefore more open to scrutiny. A great deal of research, development, and subsequent discussion surrounding actual use-cases for blockchain technology has now moved onto the role of permissioned ledgers for back-office functions in, for example, banking systems. The irony of this given the initial libertarian aspirations the technology was said to engender (*i.e.*, the avoidance of centralized financial institutions) is unmistakable. As David Golumbia remarks, this irony is symptomatic of "a reassertion of the political power that the blockchain is specifically constructed to dismantle" (David Golumbia, *The Politics of Bitcoin: Software as Right-Wing Extremism* 76 (University of Minnesota Press, 2016)); *see also*, Robert Herian, "How Blockchain Could Make Trusts More Transparent" (2016), *CoinDesk*, April 13. *https://www.coindesk.com/blockchain-trusts-more-transparent/*, accessed Jan. 16, 2018; Robert Herian, Blockchain and the Distributed Reproduction of Capitalist Class Power, in *MoneyLab Reader 2: Overcoming the Hype* 43–51 (Inte Gloerich et al. eds., Institute of Network Cultures, 2018). Moreover, as Lana Swartz has argued, the "incorprative blockchain" of back-office functions is no longer pursuing the libertarian dream of holistically remaking society, but is in in fact quite "boring" (Swartz, Lana, Blockchain Dreams: Imagining Techno-economic Alternatives after Bitcoin, in *Another Economy Is Possible*, 96 (Manuel Castells, ed., Polity Press, 2017), in the sense that it has very quickly fallen into step with the needs and desires of big business.

3. Prosser, *Supra* n.1 at 18.
4. Raz, Joseph, Liberty and Trust, in *Natural Law, Liberalism, and Morality*, 113 (Robert P. George, ed., Oxford University Press, 1996).
5. G.A. Cohen, *On the Currency of Egalitarian Justice, and Other Essays in Political Philosophy*, 217–219 (Michael Otsuka, ed., Princeton University Press, 2011); Prosser, *Supra* n.1 at 18.
6. Prosser, *Supra* n.1 at 18.
7. Iris Murdoch, *The Sovereignty of Good*, 95 (Routledge, 2001).
8. *Id.* at 95.
9. Mark Murphy, The Natural Law Tradition in Ethics. *The Stanford Encyclopaedia of Philosophy*. 2011. *https://plato.stanford.edu/entries/natural-law-ethics/*, accessed April 25, 2018.
10. *Id.*
11. Ronald Deibert & Rafal Rohozinski, Beyond Denial: Introducing Next-Generation Information Access Controls, in *Accessed Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, 10 (Ronald Deibert et al., eds., MIT Press, 2010).
12. Melanie Swan, *Blockchain: Blueprint for a New Economy*, 17 (O'Reilly, 2015).
13. *Id.* at 17.
14. Félix Guattari, *Chaosmosis: an ethico-aesthetic paradigm*, 40 (Paul Bains & Julian Pefanis, trans., Indiana University Press, 1995).
15. Michael Power, *The Audit Society: Rituals of Verification*, 7 (Oxford University Press, 1997).
16. *Id.* at 7.
17. Roger Brownsword, *Rights, Regulation, and the Technological Revolution*, 294 (Oxford University Press, 2008).
18. Ian Brown & Christopher, T. Marsden, *Regulating Code: Good Governance and Better Regulation in the Information Age* (MIT Press, 2013); Milton Mueller, *Networks and States: The Global Politics of Internet Governance* (MIT Press, 2013); Frank Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information* (Harvard University Press, 2015); Nick Srnicek, *Platform Capitalism* (Polity, 2017).
19. W. Brian Arthur, *The Nature of Technology: What It Is and How It Evolves*, 193 (Penguin, 2009).
20. Joseph A. Schumpeter, *Capitalism, Socialism and Democracy*, 73 (Routledge, 2010)—"The opening up of new markets, foreign or domestic […] a process of industrial mutation that incessantly revolutionizes the economic structure *from within*, incessantly destroying the old one, incessantly creating a new one. It is what capitalism consists in and what every capitalist concern has got to live in." [Emphasis per original]
21. Vinay Gupta. European Parliament blockchain presentation May 2017. *YouTube*. *https://www.youtube.com/watch?v=xEFVuccuHI8&t=4s*, accessed Feb. 1, 2018.
22. Don Tapscott & Alex Tapscott, *Blockchain Revolution: How the Technology behind Bitcoin Is Changing Money, Business and the World* (Portfolio Penguin, 2016).
23. Rajnish Singh. *EU must work to enable blockchain technology*. The Parliament Magazine, Nov. 7, 2017. *https://www.theparliamentmagazine.eu/articles/opinion/eu-must-work-to-enable-blockchain-technology*, accessed Mar. 31, 2018.
24. The Economist. *The trust machine*, Oct. 31–6 Nov. 6, 2015, p. 13.
25. Dirk A. Zetzsche et al., "Regulating Revolution: From Regulatory Sandboxes to Smart Regulation", 23(1) *Fordham Journal of Corporate & Financial Law*. 52 (2017).
26. *Id.* at 47–50.
27. Carla L. Reyes, "Moving Beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation: an Initial Proposal," 61(1) *Villanova Law Review*. 221 (2016).
28. The United Kingdom and European Union are both presently considering the need to regulate cryptocurrency in order to address problems of anonymity apropos money laundering and tax evasion. Other nations, South Korea for instance, are also planning to ban cryptocurrency trading for the same reasons. *See, e.g.*, Julia Kollewe, *Bitcoin: UK and EU plan crackdown amid crime and tax evasion fears*, The Guardian Dec. 4, 2017. *https://www.theguardian.com/technology/2017/dec/04/bitcoin-uk-eu-plan-cryptocurrency-price-traders-anonymity* accessed Jan. 12, 2018.
29. Angela Walch, "Blockchain's Treacherous Vocabulary: One More Challenge for Regulators," 21(2) *Journal of Internet Law*. 14 (2017).
30. The European Commission is illustrative again here, where both Eva Kaili and German EPP group MEP Jacob von Weizsäcker have backed regulatory approaches that do not "regulate too early, so as to avoid stifling innovation" (Singh, 2017).
31. Ilkka Tuomi, *Networks of Innovation: Change and Meaning in the Age of Internet*, (Oxford University Press, 2002).
32. Milton Mueller, *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace* 11 (Polity, 2017).
33. Id. at 11.
34. Arthur, *Supra* n.19 at 215; Brownsword, *Supra* n.17.
35. Tomaso Aste, et al., "Blockchain Technologies: The Foreseeable Impact on Society and Industry," 50 (9) *Computer* 18–28 (2017).
36. Stuart Hall, *Selected Political Writings: The Great Moving Right Show and Other Essays*, 318 (Sally Davison et al. eds., Duke University Press, 2017).
37. Cohen, *Supra* n.5 at 217–218.
38. *Id.* at 218.
39. *Id.* at 217–219.
40. Kai Stinchcombe, *Ten years in, nobody has come up with a use for blockchain. Hacker Noon*, Dec. 22, 2017. *https://hackernoon.com/ten-years-in-nobody-has-come-up-with-a-use-case-for-blockchain-ee98c180100*, accessed Jan. 31, 2018.
41. *https://www.fiscal.treasury.gov/fsservices/gov/fit/blockchain.htm*, accessed July 5, 2018.
42. Brown & Marsden, *Supra* n.18 at 59.
43. 2018. 25 May—GDPR tightens data protection rules for companies and gives people back control. *European Commission*. *https://ec.europa.eu/unitedkingdom/*

news/25-may-%E2%80%93-gdpr-tightens-data-protection-rules-companies-and-gives-people-back-control_en, accessed May 25, 2018.

44. Brown & Marsden, *Supra* n.18 at 59.
45. Jacek Czarnecki. *Blockchains and personal data protection regulations explained*. Coindesk, April 26, 2017. *https://www.coindesk.com/blockchains-personal-data-protection-regulations-explained/*, accessed April 20, 2018.
46. Winston Maxwell & John Salmon. *A guide to blockchain and data protection*. Hogan Lovells. September, 2017. *https://www.hlengage.com/_uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf*, accessed April 20, 2018, pp. 16–19.
47. *Id*. at 21.
48. Van Humbeeck, Andries. *The blockchain-GDPR paradox*. Medium. Nov. 21, 2017. *https://medium.com/wearetheledger/the-blockchain-gdpr-paradox-fc51e663d047*, accessed April 20, 2018.
49. *Id*
50. Maxwell & Salmon, *Supra* n.46 at 15.
51. *Id*. at 15.
52. Van Humbeeck, *Supra* n.48.
53. *Id*.
54. Stuart Biegel, *Beyond our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace*, 361 (The MIT Press, 2003).