Rules of a networked society

Dizon, M.A.

Published in:
Bridging Distances in Technology and Regulation

Publication date:
2013

Document Version
Publisher's PDF, also known as Version of record

Rules of a networked society: Here, there and everywhere

Michael Anthony C. Dizon
Tilburg University
Tilburg Institute for Law, Technology, and Society (TILT)
✉m.a.dizon@uvt.nl

Abstract With the ever-increasing informatization and technologization of society, technological rules and actors are playing a greater role in the governance of the digital and connected world. This paper argues that, in order to better understand how the networked information society is organized and operates now and in the near future, it is important to develop and adopt a pluralist, rules-based approach to the study of law and technology. This means coming to terms with and taking seriously the plural legal and extra-legal rules, norms, codes, and principles that influence behavior and determine the state and degree of normativity in society. The proposed approach can be handily applied to the case of hackers. From a pluralist perspective, hacking is not simply a problem to be solved but a complex, techno-social phenomenon that needs to be properly observed and understood. Adopting a pluralist approach to law and technology study can be valuable since multiple persons, things and rules do profoundly shape the world we live in. This rules-based approach can potentially bridge the distance between law and technology and bring them ever closer together.

Keywords rules, pluralist, normative, technology, hackers

Impact of technological rules and actors on society

At the height of the dot-com boom in the late 1990s, Lawrence Lessig expressed and popularized the idea that technical code regulates (Lessig 2006). Since then, together with rapid technological developments and widespread dissemination of technologies in all aspects of people's lives, the growing influence on the behavior of people and things of technological rules and actors other than and beyond the law and the state has become all the more apparent. The behaviors of people online are to a certain extent determined by the technical protocols and standards adopted by the Internet Engineering Task Force (IETF) and other non-governmental bodies that design the architecture of the internet (see Murray 2007, 74; Bowrey 2005, 47). The Arab Spring has proven that the use of internet-based communications and technologies can enable or have a role in dramatic political and social change (Howard 2011; Stepanova 2012).[1] Making full use of their technical proficiency, the people behind the whistleblower website Wikileaks and the hacktivist group Anonymous have become influential albeit controversial members of civil society who push the boundaries of what democracy, freedom and civil disobedience mean in a digital environment (Ludlow 2010; Hampson 2012, 512-513; Chadwick 2006, 114). Technology-related rules even had a hand in one of the most significant events of the new millennium, the Global Financial Crisis. It is claimed that misplaced reliance by financial institutions on computer models based on a mathematical algorithm (Gaussian copula function) was partly to blame for the miscalculation of risks that led to the crisis (Salmon 2009; MacKenzie&Spears 2012). The fact that a formula (i.e., a rule expressed in symbols) can affect the world in such a momentous way highlights the critical role of rules in a 'networked information society' (Cohen 2012, 3) or 'network society' (Castells 2001, 133).

[1] But see Morozov (2011a; 2011b) for more somber assessments of technology's role in political change.

This paper argues that, in order to better understand how a networked society is organized and operates now and in the near future, it is important to develop and adopt a pluralist, rules-based approach to law and technology research. This means coming to terms with and seriously examining the plural *legal and extra-legal rules*, norms, codes, and principles that influence and govern behavior in a digital and computational universe (see Dyson 2012), as well as the persons and things that create or embody these rules. Adopting this rules-based framework to technology law research is valuable since, with the increasing informatization and technologization of society (Pertiera 2010, 16), multiple actors and rules – both near and far – do profoundly shape the world we live in.

From 'what things regulate' to 'what rules influence behavior'

A pluralist and distributed approach to law and technology is not new (see Schiff Berman 2006; Hildebrandt 2008; Mifsud Bonnici 2007, 21-22 ('mesh regulation'); Dizon 2011). Lessig's theory of the four modalities of regulation (law, social norms, the market, and architecture) serves as the foundation and inspiration for many theories and conceptualizations about law, regulation and technology within and outside the field of technology law (Lessig 2006, 123; Dizon 2011). Modifying Lessig's model, Murray and Scott (2002, 492) come up with what they call the four bases of regulation: hierarchy, competition, community, and design. Similarly, Morgan and Yeung (2007, 80) advance the five classes of regulatory instruments that control behavior, namely: command, competition, consensus, communication, and code.

Lessig's conception of "*what things regulate*" (Lessig 2006, 120) is indeed insightful and useful for thinking about law and technology in a networked society. I contend, however, that his theory can be remade and improved by: (1) modifying two of the modalities; (2) moving away from the predominantly instrumentalist concerns of 'regulation' and how people and things can be effectively steered and controlled to achieve stated ends (Morgan & Yeung 2007, 3-5; Black 2002, 23, 26); and (3) focusing more on how things actually influence behavior rather than just how they can be regulated. I prefer to use the term 'technology' rather than 'architecture' since the former is a broader concept that subsumes architecture and code within its scope. By technology, I mean the '*application of knowledge to production from the material world. Technology involves the creation of material instruments (such as machines) used in human interaction with nature*' (Giddens 2009, 1135). The regulatory modality of 'the market' is slightly narrow in its scope since it pertains primarily to the results of people's actions and interactions. This modality can be expanded to also cover the 'naturaland social forces and occurrences' (including economic ones) that are present in the physical and material world. In the same way that market forces have been the classic subject of law and economics, it makes sense for those studying law and technology issues to also examine other scientific phenomena. As will be explained in more detail below, social norms are distinguished from natural and social phenomena since the former are composed of prescriptive (ought) rules while the latter are expressed as descriptive (is) rules. Based on the above conceptual changes to Lessig's theory, the *four things that influence behavior* are: (1) law, (2) norms, (3) technology, and (4) natural and social forces and occurrences.

The four things that influence behavior can be further described and analyzed in terms of the rules that constitute them. From a rules-based perspective, law can be conceived of as being made up of *legal rules*, and norms are composed of specific *social norms*. On their part, technolo-

gy consists of *technical codes and instructions*, while natural and social forces and occurrences are expressed in *scientific principles and theories*. By looking at *what rules influence behavior*, one can gain a more detailed, systematic and interconnected picture of who and what governs a networked society. Lessig's well-known diagram of what constrains an actor can be reconfigured according to the four types of rules that influence behavior. The *four rules of a networked society* therefore are *legal rules*, *social norms*, *technical codes*, and *scientific principles* (see Figure 1).

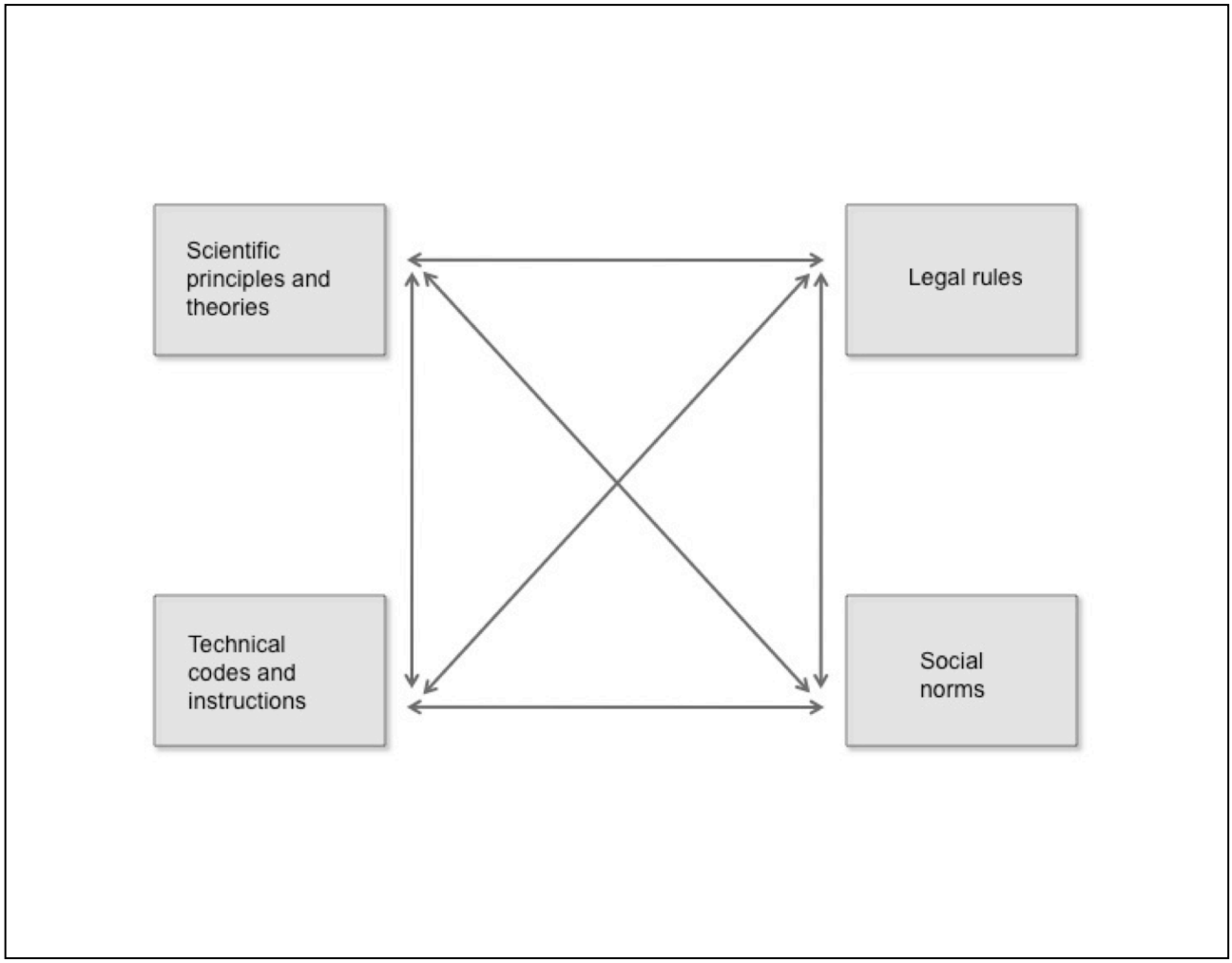

Figure 1: The four rules of a networked society

Rules of a networked society

Plurality of rules

How the various rules of a networked society relate to and interact with each other is very important to understanding how the informational and technological world works. Having a clear idea of how and why the rules are distinct yet connected to one another is paramount given that, in most cases, there are multiple overlaps, connections, intersections and even conflicts among these rules. More often than not, *not one but many rules* are present and impact behavior in any given situation.

The presence of two or more rules or types of rules that influence behavior in a given situation gives rise to a condition of *plurality of rules*. Plurality of rules resembles the concept of 'legal pluralism', which is described by John Griffiths as "*that state of affairs, for any social field, in which behavior pursuant to more than one legal order occurs*" (Griffiths 1986, 2; von Benda-Beckmann & von Benda-Beckmann 2006, 14). Legal pluralism generally considers both descriptive and normative/prescriptive rules as falling within the ambit of the term law (von Benda-Beckmann 2002, 48). As a result, legal pluralism has been subject to the perennial criticism that, due to its more expansive conception of law, the distinction between law and other forms of social control has been blurred (Merry 1988, 871, 878-879, 858; Griffiths 1986, 307; von Benda-Beckmann 2002, 47, 54, 56). In order to avoid a similar critique, while still maintaining a pluralist perspective, I deliberately use the term 'rule' (*regula*) rather than 'law' (*lex*) to characterize and describe the things that influence and govern behavior. Unlike law, which is inherently normative, a rule has greater flexibility and can cover both is and ought statements. In this way, the important distinction between descriptive rules and normative rules is retained, and the term rule can still be used in two discrete senses: (1) as an observed *regularity*[2] and (2) as a *standard* that must be observed. The concept of rules is thus sufficiently robust and nuanced that it can serve as the basis for constructing a new way of perceiving the state and degree of normativity in the networked information society (Riesenfeld 2010). Far from conflating the four things that influence behavior, a rules-based perspective is able to integrate and find important interconnections between and among them while, at the same time, preserving and taking in account their uniqueness.

The different types of rules of a networked society and how they connect with each other are explained in greater detail below.

Legal rules and social norms

Legal rules and social norms are both prescriptive types of rules. A social norm has been defined in a number ways: as 'a statement made by a number of members of a group, not necessarily by all of them, that the members ought to behave in a certain way in certain circumstances' (Opp 2001, 10714), as 'a belief shared to some extent by members of a social unit as to what conduct *ought to be* in particular situations or circumstances' (Gibbs 1966, 7), and as 'generally accepted, sanctioned prescriptions for, or prohibitions against, others' behavior, belief, or feeling, i.e. what others *ought* to do, believe, feel – *or else*' (Morris 1956, 610). Dohrenwend proffers a more detailed definition:

> A social norm is a rule which, over a period of time, proves binding on the overt behavior of each individual in an aggregate of two or more individuals. It is marked by the following characteristics: (1) Being a rule, it has content known to at least one member of the social aggregate. (2) Being a binding rule, it regulates the behavior of any given individual in the social aggregate by virtue of (a) his having internalized the rule; (b) external sanctions in support of the rule applied to him by one or more other individuals in the social aggregate; (c) external sanctions in support of the rule applied to him by an authority outside the social aggregate; or any combination of these circumstances. (Dohrenwend 1959, 470)

From the above definitions, the attributes of social norms are: '*(1) a collective evaluation of behavior in terms of what it* ***ought to be****; (2) a collective expectation as to what behavior* ***will be****; and/or*

[2] In relation to social norms, behavioral regularities that lack a normative element are also called "conventions" (see McAdams & Rasmusen 2007, 1576).

*(3) particular **reactions** to behavior, including attempts to apply sanctions or otherwise induce a particular kind of conduct*'. (Gibbs 1965, 589)

Norms are a key element to a rules-based approach to law and technology. This is especially evident when one recognizes that law is '*a type of norm*' and '*a subset of norms*' (Gibbs 1966, 315; Opp 2001, 10715; Posner 1997, 365[3]) Laws may be deemed to be more formal norms. Galligan holds the inverse to be true: '*some rule-based associations are mirrors of law and as such may lay some claim to be considered orders of **informal laws***' (Galligan 2007, 188). Norms and laws can therefore be imagined as forming a *continuum* and the degree of formality, generality, certainty and importance (among other things) is what moves a rule of behavior from the side of norms to the side of law (see Ruby 1986, 591).

Legal rules and social norms have a close and symbiotic relationship. Cooter explains one of the basic dynamics of laws and norms, '*law can grow from the bottom up by [building upon and] enforcing social norms*' (Cooter 1996, 947-948), but it can also influence social norms from the top down – "*law may improve the situation by enforcing a beneficial social norm, suppressing a harmful social norm, or supplying a missing obligation*" (ibid 1996, 949). Traditional legal theory has settled explanations of how laws and norms interact. Social norms can be transformed into legal norms or accorded legal status by the state through a number of ways: incorporation (social norms are transformed or codified into law by way of formal legislative or judicial processes), deference (the state recognizes social norms as facts and does not interfere with certain private transactions and private orderings), delegation (the state acknowledges acts of self-regulation of certain groups) (Michaels 2005, 1228, 1231, 1233 and 1234), and recognition (the state recognizes certain customary or religious norms as state law) (van der Hof & Stuurman 2006, 217).

Technical codes and instructions

Technical codes like computer programs consist of descriptive rather than prescriptive instructions. However, the value of focusing on rules of behavior is that the *normative effects* of technical codes can be fully recognized and appreciated. Despite the title of his seminal book and his famous pronouncement that '*code is law*', Lessig (2006, 5) does not actually consider technical or computer code to be an actual category or form of law, and the statement is basically an acknowledgement of code's law-like properties. As Leenes (2011, 145) points out, '*Although Lessig states that 'code is law', he does not mean it in a literal sense*'. Even Reidenberg's earlier concept of Lex Informatica, which inspired Lessig, is law in name only (Lessig 2006, 5). Reidenberg explicitly states that Lex Informatica can be '*a useful **extra-legal** instrument that may be used to achieve objectives that otherwise challenge conventional laws and attempts by government to regulate across jurisdictional lines*' (1997, 556 emphasis added). While Lex Informatica '*has analogs for the key elements of a legal regime*', it is still '*a **parallel rule system***' that is '*distinct from legal regulation*' (Reidenberg 1997, 569, 580 emphasis added). But if '*code is not law*' as some legal scholars conclude (Dommering 2006, 11, 14), what exactly is the relationship between technical codes and law, and what is the significance of code in the shaping of behavior in a networked society?

Using the above definition and characterization of norms, technical code *in and of itself* (i.e., excluding any such norms and values that an engineer or programmer intentionally or unintention-

[3] "law is older than political society, which means that it originates as a set of norms" Posner (2000, 365).

ally implements or embodies in the instructions) is *neither a legal rule nor a social norm* because: (1) it is not a shared belief among the members of a unit; (2) there is no *oughtness* (must or should) or a sense of obligation or *bindingness* in the *if-then* statements of technical code (they are simply binary choices of on or off, true or false, is versus not); (3) there is no 'or else' element that proceeds from the threat of sanctions (or the promise of incentives) for not conforming (or conforming) with the norm; (4) the outcome of an if-then statement does not normally call for the imposition of external sanctions by an authority outside of the subject technology; (5) and, generally, there is no collective evaluation or expectation within the technical code itself of what the behavior ought to be or will be (a matter of *is* and not *ought*).

Even though technical codes and instructions are not per se norms, they can undoubtedly have normative effects (van der Hof & Stuurman 2006, 218, 227). Furthermore, technologies are socially constructed and can embody various norms and values (Pinch & Bijker 1984, 404). A massively multiplayer online role-playing game (MMORPG) such as World of Warcraft has its own rules of play and can, to a certain extent, have normative effects on the persons playing it (they must abide by the game's rules and mechanics). A virulent computer program such as the 'ILOVEYOU' virus/worm (or the Love Bug) that caused great damage to computers and IT systems around the world in 2000 can have a strong normative impact; it can change the outlooks and behaviors of various actors and entities (Cesare 2001, 145; Grossman 2000). As a result of the outbreak of the Love Bug, employees and private users were advised through their corporate computer policies or in public awareness campaigns not to open email attachments from untrustworthy sources. In the Philippines, where the alleged author of the Love Bug resided, the Philippine Congress finally enacted a long awaited Philippine Electronic Commerce Act, which contained provisions that criminalized hacking and the release of computer viruses.[4] The Love Bug, which is made up of technical instructions, definitely had a strong normative impact on computer use and security.

Digital rights management (DRM) is an interesting illustration of the normative effects of technology since, in this case, technical code and legal rules act together to enforce certain rights for the benefit of content owners and limit what users can do with digital works and devices (see Brown 2006). DRM on a computer game, for example, can prevent users from installing or playing it on more than one device. Through the making of computer code, content owners are able to create and grant themselves what are essentially new and expanded rights over intellectual creations that go beyond the protections provided to them under intellectual property laws (van der Hof & Stuurman 2006, 215; McCullagh 2005). Moreover, supported by both international and national laws,[5] DRM acts as hybrid techno-legal rules that not only restrict the ability of users to access and use digital works wrapped in copy protection mechanisms, but the circumvention of DRM and the dissemination of information about circumvention techniques are subject to legal sanctions (see Dizon 2010).[6] When users across the world play a computer game with 'always-on' DRM like

---

4 Philippine Electronic Commerce Act, s 33(a); Disini, Jr. & Toral (2000, 36-37; Sprinkel 2001, 493-494; Pabico & Chua 2001).

5 See WIPO Copyright Treaty and the World Performance and Phonograms Treaty (together the WIPO Internet Treaties).

6 Another noteworthy example of hybrid techno-legal rules are those relating to "privacy by design", which are being advanced in the privacy and data protection regulations of Canada and the European Union (see Cavoukian 2009; see European Commission COM(2010) 245 final/2 and COM(2010) 609 final.

Ubisoft's *Driver*, it is tantamount to people's behavior being subjected to a kind of transnational, technological control, which users have historically revolted against (Hutchinson 2012; Doctorow 2008).

Another example of hybrid techno-legal rules is the so-called Great Firewall of China. This computer system that monitors and controls what users and computers within China can access and connect to online clearly has normative effects since it determines the actions and communications of an entire population (Karagiannopoulos 2012, 155). In fact, it does not only control what can be done within China but it also affects people and computers all over the world (e.g., it can prevent a Dutch blogger or a U.S. internet service such as YouTube from communicating with Chinese users and computers). In light of their far-reaching normative impact, technical codes and instructions should not be seen as mere instruments or tools of law (Dommering 2006, 13-14), but as a distinct type of rule in a networked society. Code deserves serious attention and careful consideration in its own right.

Scientific principles and theories

There is a whole host of scientific principles, theories and rules from the natural, social and formal sciences that describe and explain various natural and social phenomena that influence the behavior of people and things. Some of these scientific principles are extremely relevant to understanding the inner workings of a networked society. For example, Moore's Law is the observation-cum-prediction of Intel's co-founder Gordon Moore that '*the number of transistors on a chip roughly doubles every two years*',[7] and can be expressed in the mathematical formula $n = 2^{((y - 1959) \div d)}$ (Ceruzi 2005, 585)[8] Since 1965, this principle and the things that it represents have shaped and continue to profoundly influence all aspects of the computing industry and digital culture particularly what products and services are produced and what people can or cannot do with computers and electronic devices (Ceruzzi 2005, 586; Hammond 2004; see Anderson 2012, 73, 141). Ceruzzi rightly claims, '*Moore's law plays a significant role in determining the current place of technology in society*' (2005, 586). However, it is important to point out that Moore's Law is not about physics; it is a self-fulfilling prophecy that is derived from 'the confluence and aggregation of individuals' expectations manifested in organizational and social systems which serve to self-reinforce the fulfillment of Moore's prediction' for some doubling period (Hammond 2004, citations omitted)and is '*an emergent property of the highly complex organization called the semiconductor industry*' (ibidem). This statement reveals an important aspect of Moore's Law and other scientific principles and rules – that they are also *subject to social construction*. As Jasanoff eruditely explains:

> science is *socially constructed*. According to a persuasive body of work, the "facts" that scientists present to the rest of the world are not simple reflections of nature; rather these "facts" are produced by human agency, through the institutions and processes of science, hence they invariably contain a social component. Facts, in other words, are more than merely raw observations made by scientists exploring the mysteries of nature. Observations achieve the status of "facts" only if they are produced in accordance with prior agreements about the rightness of particular theories, experimental methods, instrumental techniques, validation procedures, review processes, and the like. These agreements, in turn, are socially de-

7 <http://download.intel.com/museum/Moores_Law/Printed_Materials/Moores_Law_2pg.pdf> accessed 7 September 2012;see also Ceruzzi (2005, 584).

8 n is the number of circuits, y is the current year and d is the doubling time.

rived through continual negotiation and renegotiation among relevant bodies of scientists (Jasanoff 1991, 347; see also Polanyi 2000).

Since the construction of scientific rules and facts is undertaken by both science and non-science institutions, "what finally counts as 'science' is influenced not only by the consensus views of scientists, but also by society's views of what nature is like – views that may be conditioned in turn by deep-seated cultural biases about what nature should be like" (Jasanoff 1991, 347). Due to "the contingency and indeterminacy of knowledge, the multiplicity and non-linearity of 'causes', and the importance of the narrator's (or the scientific claims-maker's) social and cultural standpoint in presenting particular explanations as authoritative" (Jasanoff 1996, 411-412), science is without doubt a 'deeply political' and 'deeply normative' activity (Jasanoff 1996, 409, 413; see Geertz 1983, 189; Hoppe 1999). It reveals as much about us as it does the material world.

The 'constructedness' (Jasanoff 1991, 349) of science can also been seen in the history of the use of and meaning ascribed to the term 'scientific law'. The use of the term 'law' in reference to natural phenomena has been explained as '*a metaphor of divine legislation*", which "*combined the biblical ideas of God's legislating for nature with the basic idea of physical regularities and quantitative rules of operation*' (Ruby 1986, 341, 342,358 (citations omitted). Ruby argues, however, that the origins of the use of the term law (*lex*) for scientific principles is not metaphorical but is inherently connected to the use and development of another term, rule (*regula*) (Ruby 1986, 347, 350). Through the changing uses and meanings of *lex* and *regula* and their descriptive and/or prescriptive application to the actions of both man and nature throughout the centuries, law in the field of science became more commonly used to designate a more fundamental or forceful type of rule, which nevertheless pertains to some 'regularity' in nature. At its core, a scientific principle or law is about imagining '*nature as a set of intelligible, measurable, predictable* ***regularities***' (Ruby 1986, 350 (emphasis added)).

Another important characteristic of scientific principles is that they act as signs, and consist of both signifier and signified. Moore's Law is both the expression and the embodiment of the natural and social forces and occurrences that it describes. As Ruby (1986, 347) explains, "*in the case of natural phenomena it is not always possible to distinguish the use of lex for formulated principles from that for regularities in nature itself*". Thus, from a practical standpoint, natural and social phenomena are reified and can be referred to by the labels and formulations of the relevant scientific principles that they are known by. For example, rather than saying, 'the forces described by Moore's Law affected the computer industry', it can be stated simply as 'Moore's Law affected the computer industry'.

There is much that can be learned about how the world works if we take as seriously the influence of scientific rules on behavior as we do legal ones. Scientific principles are descriptive and not prescriptive rules, but, like technical codes, they too are socially constructed and have significant normative effects on society and technology, and are thus worth studying in earnest (see Jasanoff 1996, 397 'co-production of scientific and social order'). People who are aware of the descriptive 'theory of the Long Tail' (Anderson 2007, 52)[9] would *conform* their actions to this rule and build

[9] The Long Tail is the phenomenon where consumption and production "are increasingly shifting away from a focus on a relatively small number of hits (mainstream products and markets) at the head of the demand curve, and moving towards a huge number of niches in the tail".

businesses that answer the demands of niche markets. Scientists and engineers are obviously cognizant of the "law of gravity" and they know that they *ought* to design rockets and airplanes based on this important descriptive principle. Competition authorities know that they *must* take into account market forces and relevant economic principles before imposing prescriptive rules on a subject entity or market. These and many other examples show how descriptive rules can also give rise to or be the basis of ought actions and statements.[10] Descriptive rules as such can influence behavior and have normative effects.

Being able to incorporate scientific principles within the purview of law and technology research is important since it creates connections that bring the fields of law and science and technology ever closer together. If there is value in a sociologist of science and technology studying law-making processes (Latour 2010), there is equal merit in law and technology researchers examining scientific principles and technical codes since rules that govern the networked society can similarly be made and found in laboratories and workshops (Latour 2010; Callon 1987, 99).

Significance of rules

On a theoretical level, a rules-based approach is very useful and valuable to law and technology research in a number of ways. First, it distinguishes but does not discriminate between normative and descriptive rules. While the key distinction between is and ought is maintained, the role and impact of descriptive rules on behavior and order is not disregarded but is, in fact, fully taken into account. By focusing as well on descriptive rules and regularities that are not completely subject to human direction, a rules-based framework can complement and support the more instrumentalist, cybernetic and state-centric theories and methods to law and technology (Morgan & Yeung 2007, 3-5, Black 2002, 23, 26). Rather than concentrating solely or mainly on how state actors and the law directly or indirectly regulate behavior, a rules-based approach creates an awareness that problems and issues brought about by social and technological changes are often not completely solvable through man-made, top-down solutions alone, and more organic and bottom-up approaches should also be pursued. By placing equal emphasis on descriptive rules such as technical codes and scientific principles and their normative effects, the complexity and unpredictability of reality can be better understood, and the people, things and phenomena within and beyond our control are properly considered, addressed or, in some case, left alone.

Second, conceptualizing the networked society in terms of is and ought rules makes evident the 'duality of structure' that recursively constitutes and shapes our world (Giddens 1984 25, 375). As Giddens explains,

> The constitution of agents and structures are not two independently given set of phenomena, a dualism, but represent a duality. According to the notion of duality of structure, the structural properties of social systems are both medium and outcome of the practices they recursively organized. Structure is not "external" to individuals…. Structure is not to be equated with constraint but is always both constraining and enabling. (Giddens 1984, 25)

Applying Giddens' 'theory of structuration', a networked society is thus not constituted solely by one dimension to the exclusion of another – agency versus structure, human against machine,

[10] Hume's law, which states that one cannot derive ought from is, is not applicable since the examples do not involve morality but conclusions based on experience and empirical data (see Hume (1739, Book III, Part I, Section 1)).

man versus nature, instrumentalism or technological determinism, society or technology – but it is the action-outcome of the mutual shaping of any or all of these dualities (Giddens 1984).

Finally, a rule can be a key concept for an interdisciplinary approach to understanding law, technology and society. A rule can serve as a common concept, element or interface that connects and binds different academic fields and disciplines (Therborn 2002, 863). With the increasing convergence of different technologies and various fields of human activity (both inter and intra) and the multidisciplinary perspectives demanded of research today, a unifying concept can be theoretically and methodologically useful. The study of rules (particularly norms) has received serious attention from such diverse fields as law (see Posner 2000; Sunstein 1996; Lessig 1995; Cooter 2000), sociology (Hecter 2001), economics (McAdams & Rasmusen 2007; Posner 1997), game theory (Bicchieri 2006; Axelrod 1986), and even information theory (Boella et al. 2006; Floridi 2012). The study of '*normative multiagent systems*' illustrates the interesting confluence of issues pertaining to law, technology and society under the rubric of rules (Boella et al. 2006; Savarimuthu & Cranefield 2011).

Rules of hacking

In addition to its conceptual advantages, a rules-based approach can be readily applied to analyze real world legal and normative problems that arise from technical and social changes. There can be greater clarity in determining what issues are involved and what possible actions to take when one perceives the world as being '*normatively full*' (Griffiths 2002, 34) and replete with rules. For instance, the 'problem' of computer hacking[11] is one that legislators and other state actors have been struggling with ever since computers became widely used. Using the rules of a networked society as a framework for analysis, it becomes evident that hacking is not simply a problem to be solved but a complex, techno-social phenomenon that needs to be properly observed and understood.

Laws on hacking

Early attempts to regulate hacking seemingly labored under the impression that the only rules that applied were legal rules. Thus, despite the absence of empirical data showing that hacking was an actual and serious threat to society, legislators around the world enacted computer fraud and misuse statutes that criminalized various acts of hacking, particularly unauthorized access to a computer (Hollinger 1991, 8). Some studies have shown, however, that these anti-hacking statutes have mostly been used against disloyal and disgruntled employees and only seldom in relation to anonymous outsiders who break into a company's computer system, the oft-cited bogeyman of computer abuse laws (Hollinger 1991, 9; Skibbel 2003, 918). Not all laws though are opposed to all forms of hacking. The Software Directive upholds the rights to reverse engineer and to decompile computer programs to ensure interoperability subject to certain requirements.[12] The fair use doc-

[11] To "hack" is to produce a surprising result through deceptively simple means, which belies the impressive mastery or expertise possessed by an actor who is neither bound nor excluded by the rules of the subject technology or technological system. This is a paraphrasing and refinement of Turkle definition of a hack (see Turkle 2005, 208).

[12] Directive 2009/24/EC of 23 April 2009 on the legal protection of computer programs [2009] OJ L111/416, art 5(3), 6, and 8.

trine and similar limitations to copyright provide users and developers with a bit of (but clearly not much) space and freedom to hack and innovate (see Rogers & Szamosszegi 2011).

Norms of hackers

Another thing that state actors fail to consider when dealing with hacking is that computer hackers belong to a distinct culture with its own set of rules. Since the social norms and values of hackers are deeply held, the simple expedient of labeling hacking as illegal or deviant is not sufficient to deter hackers from engaging in these legally prohibited activities. In his book *Hackers*, Levy codified some of the most important norms and values that make up the hacker ethic:

- Access to computers should be unlimited and total.
- All information should be free.
- Mistrust Authority – Promote Decentralization.
- Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.
- You can create art and beauty on a computer.
- Computers can change your life for the better (Levy 2010, 28-34).

These norms and values lie at the very heart of hacker culture and are a source from which hackers construct their identity. Therborn (2002, 869) explains the role of norms in identity formation, "*This is not just a question of an 'internalization' of a norm, but above all a linking of our individual sense of self to the norm source. The latter then provides the meaning of our life*". While hacker norms have an obviously liberal and anti-establishment inclination, the main purposes of hacking are generally positive and socially acceptable (e.g., freedom of access, openness, freedom of expression, autonomy, equality, personal growth, and community development). It is not discounted that there are hackers who commit criminal acts and cause damage to property. However, the fear or belief that hacking is intrinsically malicious or destructive is not supported by hacker norms. In truth, many computer hackers adhere to the rule not to cause damage to property and to others (Levy 2010, 457). Among the original computer hackers in the Massachusetts Institute of Technology (MIT) and the many other types and groups of hackers, there is a '*cultural taboo against malicious behavior*' (Williams 2002, 178). Even the world famous hacker Kevin Mitnick, who has been unfairly labeled as a '*dark-side hacker*' (Hafner & Markoff 1991, 15), never hacked for financial or commercial gain (Mitnick & Siomon 2011; Hollinger 2001, 79; Coleman & Golub 2008, 266).

It is not surprising then that the outlawing and demonization of hacking inflamed rather than suppressed the activities of hackers. After his arrest in 1986, a hacker who went by the pseudonym of The Mentor wrote a hacker manifesto that was published in Phrack, a magazine for hackers, and became a rallying call for the community.[13] The so-called 'hacker crackdown' in 1990 (also known as Operation Sun Devil, where U.S. state and federal law enforcement agencies attempted to shut down rogue bulletin boards run by hackers that were allegedly "*trading in stolen long distance telephone access codes and credit card numbers*") (Hollinger 2001, 79) had the unintended effect of spurring the formation of the Electronic Frontier Foundation, an organization of digital

[13] The Mentor, "The Hacker Manifesto" <http://www.phrack.org/issues.html?issue=7&id=3> accessed 4 December 2012.

rights advocates (Sterling 1992, 12). Similarly, the suicide of a well-known hacker, Aaron Schwartz, who at the time of his death was being prosecuted by the US Justice Department for acts of hacktivism, has spurred a campaign to finally reform problematic and excessively harsh US anti-hacking statutes that have been in force for decades.[14]

It may be argued that Levy's book, which is considered by some to be the definitive account of hacker culture and its early history, was a response of the hacker community (with the assistance of a sympathetic journalist) to counteract the negative portrayal of hackers in the mass media and to set the record straight about the true meaning of hacking (Levy 2010, 456-457, 464; Sterling 1992, 57, 59; Coleman & Golub 2008, 255). Through Levy's book and most especially his distillation of the hacker ethic, hackers were able to affirm their values and establish a sense of identity and community (Williams 2002, 177-178). According to Jordan and Taylor,

> Rather than hackers learning the tenets of the hacker ethic, as seminally defined by Steven Levy, they negotiate a common understanding of the meaning of hacking of which the hacker ethic provides a ready articulation. Many see the hacker ethic as a foundation of the hacker community. (Jordan & Taylor 2008, 774-775)

To illustrate the importance of Levy's book as a statement for and about hacker culture, the well-known German hacker group Chaos Computer Club uses the hacker ethic as their own standards of behavior (with a few additions).[15]

Technologies of hacking

Hackers do not only practice and live out their social norms and values, but the latter are embodied and upheld in the technologies and technical codes that hackers make and use. This is expected since hackers possess the technical means and expertise to route around, deflect or defeat the legal and extra-legal rules that challenge or undermine their norms. Sterling notes, "*Devices, laws, or systems that forbid access, and the free spread of knowledge, are provocations that any free and self-respecting hacker should relentlessly attack*" (1992, 66). The resort of hackers to technological workarounds is another reason why anti-hacking laws have not been very successful in deterring hackingactivities.

Despite the legal prohibition against different forms of hacking, there is a whole arsenal of tools and techniques that are available to hackers for breaking and making things. There is not enough space in this paper to discuss in detail all of these hacker tools, but the following are some technologies that clearly manifest and advance hacker norms. Free and open source software (FOSS) is a prime example of value-laden hacker technology (Coleman & Golub 2008, 262). FOSS is a type of software program that is covered by a license that allows users and third party developers the rights to freely run, access, redistribute, and modify the program (especially its source code).[16] FOSS such as Linux (computer operating system), Apache (web server software), MySQL

---

14 Electronic Frontier Foundation, "Computer Fraud And Abuse Act Reform" <https://www.eff.org/issues/cfaa> accessed 4 March 2013; see Olivenbaum (1996).

15 See Chaos Computer Club, "hackerethics" <http://www.ccc.de/hackerethics> accessed 7 November 2012

16 Free Software Foundation, "What is free software?" <http://www.gnu.org/philosophy/free-sw.html> accessed 5 December 2012; Open Source Initiative, "The Open Source Definition" <http://opensource.org/osd> accessed 5 December 2012.

(database software) WordPress (content management system), and Android (mobile operating system) are market leaders in their respective sectors and they exert a strong influence on the information technology industry as a whole. The freedoms or rights granted by FOSS licenses advance the ideals of free access to computers and freedom information, which arealso the first tenets of the hacker ethic. What is noteworthy about FOSS and its related licenses is that they too are a convergence of legal rules (copyright and contract law), social norms (hacker values), technical codes (software) and scientific principles (information theory) (Coleman 2009; Benkler 2006, 60). In order to grasp the full meaning and impact of FOSS on society, one mustengage with the attendant plurality of rules. Other noteworthy examples of hacking technologies that hackers use with higher socio-political purposes in mind are Pretty Good Privacy (PGP, an encryption program for secret and secure communications) (Coleman & Golub 2008, 259), BackTrack (security auditing software that includes penetration testing of computer systems), Low Orbit Ion Cannon (LOIC, network stress testing software that can also be used to perform denial-of-service attacks), and circumvention tools such as DeCSS (a computer program that can decrypt content that is protected by a technology protection measure).

Technical codes are an important consideration in the governance of a networked society since "technology is not a means to an end for hackers, it is central to their sense of self – making and using technology is how hackers individually create and how they socially make and reproduce themselves" (Coleman & Golub 2008, 271). While technical codes are not themselves norms, they can embody norms and have normative effects. As such, technical codes too are essential to understanding normativity in a networked society.

Science of hacking

The norms and normative effects of hacking tend to be supported and often magnified by scientific principles and theories. Hackers, for instance, can rely on Moore's Law and the principle of 'economies of scale' (Lemley & McGowan 1998, 494) to plan for and develop technologies that are exponentially faster and cheaper, which can receive the widest distribution possible. Being cognizant of Schumpeter's 'process of creative destruction' (Schumpeter 1962) and Christensen's related 'theory of disruptive innovation' (Christensen 2006), hackers, as innovators and early adopters of technology, are in an ideal position to take advantage of these principles and create new technologies or popularize the use of technologies that can potentially challenge or upend established industries. Creative destruction is Schumpeter's theory that capitalist society is subject to an evolutionary process that "*incessantly revolutionizes the economic structure* ***from within****, incessantly destroying the old one, incessantly creating a new one*" (Schumpeter 1962, 82). Schumpeter argues that today's monopolists industries and oligopolistic actors will naturally and inevitably be destroyed and replaced as a result of competition from new technologies, new goods, new methods of production, or new forms of industrial organization (Schumpeter 1962, 82-83). The revolutionary Apple II personal computer, the widely used Linux open source operating system, the controversial BitTorrent file-sharing protocol, and the ubiquitous World Wide Web are some notable technologies developed by hackers,[17] which through the process of creative destruction profoundly changed not

[17] Steve Wozniak, Linus Torvalds, Bram Cohen, and Tim Berners-Lee, creators of the Apple II, Linux, BitTorrent and the World Wide Web, respectively, view themselves as hackers and participate in hacker culture (see Levy 2010, 249; see Himanen 2001; see Thompson 2005; see Berners-Lee 2013).

just the economic but the legal, social and technological structures of the networked society as well.

Furthermore, because of their proclivity for open standards, resources and platforms that anyone can freely use and build on, hackers can naturally benefit from principles of network theory such as network effects. According to Lemley,

> "Network effects" refers to a group of theories clustered around the question whether and to what extent standard economic theory must be altered in cases in which "the utility that a user derives from consumption of a good increases with the number of other agents consuming the good." (Lemley & McGowan 1998, 483 (citations omitted))

This means that the more people use a technology, the greater the value they receive from it and the less likely they will use another competing technology. A consequence of network effects is a

> natural tendency toward de facto standardization, which means everyone using the same system. Because of the strong positive-feedback elements, systems markets are especially prone to 'tipping,' which is the tendency of one system to pull away from its rivals in popularity once it has gained an initial edge (Lemley & McGowan 1998, 483 (citations omitted)).

Network effects and the openness of the Android open source mobile operating system may partly explain how Android became dominant in the smartphone market despite the early lead of Apple's iPhone and iOS. While Apple's iOS operating system is proprietary, closed and can only be used on Apple's own devices, developers are free to use, modify and improve the open source software components of Android, and manufacturers can use Android on their devices subject to certain limitations. The success of Android confirms a view that hackers will have no trouble agreeing with – "*open always wins… eventually*" (Downes 2009).

Creative destruction and network effects are a few of the important scientific principles and theories that influence the networked information society that hackers are able to benefit from. These principles do not merely remain in the background, quietly establishing the conditions and contexts of action, but, as cognitive statements about observed phenomena in nature and the market, they have strong normative effects in their own right and people tend to conform their behavior to these principles.

Rules, rules everywhere

As illustrated in the case of hacking, a pluralist and rules-based approach can be very useful in describing and analyzing legal problems and normative issues brought about by new or disruptive technologies. Attempts by state and non-state actors to adapt to the changing digital environment or to change people's behaviors can derive much benefit from knowing how the world works. The workings of the networked society can be framed in infinite ways, but, as explained above, seeing these operations in relation to the presence, action and interaction of rules is extremely helpful in making sense of reality. The formation and implementation of laws must therefore take into account the social, technical and scientific rules that govern a subject area or field. This is necessary because behavior in a technology-mediated and scientifically validated world is not only shaped by laws, but equally by norms, technologies, and natural and social phenomena. These four rules, whether as norms as such or through their normative effects, determine the state and degree of normativity in a networked society.

This paper has enlarged the domain of technology law to cover not just legal rules but also extra-legal rules such as social norms, technical code, and scientific principles. The expanded scope should not be bemoaned but instead embraced as a challenge since there are now more interesting people, things and phenomena which technology lawyers and legal scholars can and ought to study. There is nothing wrong with perceiving the networked society in relation to rules. Other academic fields have no problem seeing the world through their own distinct and widely-encompassing disciplinary lenses – for anthropologists it is all about culture, evolutionary biologist focus on the gene, physicists perceive the universe in terms of matter and energy, and information theorists unabashedly see everything as bits. Technology law researchers should not hesitate to say that everything could potentially be about rules. In a world where normative and descriptive rules pervade all aspects of our lives and we have to constantly negotiate all sorts of rules, norms, codes and principles, a pluralist and rules-based approach brings law and technology study much closer to the messy reality that it seeks to understand and explain. Just look around and it is evident that the world is truly normatively complex and full of rules.

References

Anderson, Chris (2007). The Long Tail: How Endless Choice is Creating Unlimited Demand, Random House Business Books.

Anderson, Chris (2012). *Makers: The New Industrial Revolution,* Random House Business Books.

Axelrod, Robert (1986). "An Evolutionary Approach to Norms", 80 *American Political Science Review,* 1095.

Benkler, Yochai (2006). The Wealth of Networks: How Social Production Transforms Markets and Freedom, Yale University Press.

Berman, Paul Schiff (2006). "Global Legal Pluralism", 80 *Southern California Law Review* 1155.

Berners-Lee, Tim (2013). "Aaron is dead" W3C mailing list <http://lists.w3.org/Archives/Public/www-tag/2013Jan/0017.html> accessed 4 March 2013.

Bicchieri, Cristina (2006). The Grammar of Society: The Nature and Dynamics of Social Norms, Cambridge University Press.

Black, Julia (2002). "Critical Reflections on Regulation", 27 *Australian Journal of Legal Philosophy* 1.

Boella, Guido, Leendert van der Torre and Harko Verhagen (2006). "Introduction to normative multiagent systems", 12 *Computation & Mathematical Organization Theory* 71.

Bowrey, Kathy (2005). *Law and Internet Cultures,* Cambridge University Press 2005.

Brown, Ian (2006). "The Evolution of Anti-Circumvention Law", 20 *International Review of Law, Computers & Technology* 239.

Callon, Michel (1987). "Society in the Making: The Study of Technology as a Tool for Sociological Analysis" in WE Bijker, TP Hughes and TJ Pinch (eds), *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*, The MIT Press.

Castells, Manuel (2001). The Internet Galaxy: Reflections on the Internet, Business, and Society, Oxford University Press.

Cavoukian, Ann (2009). "Privacy by Design: The 7 Foundational Principles" <http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf> accessed 4 March 2013.

Ceruzzi, Paul E. (2005). “Moore's Law and Technological Determinism”, 46 *Technology and Culture* 584.

Cesare, Kelly (2001). “Prosecuting Computer Virus Authors: The Need for an Adequate and Immediate International Solution”, 14 *The Transnational Lawyer* 135.

Chadwick, Andrew (2006). Internet Politics: States, Citizens, and New Communication Technologies, Oxford University Press.

Chaos Computer Club, “hackerethics” <http://www.ccc.de/hackerethics> accessed 7 November 2012.

Christensen, Clayton M. (2006). “The Ongoing Process of Building a Theory of Disruption”, 23 *The Journal of Product Innovation Management* 39.

Cohen, Julie E. (2012). Configuring the Networked Self: Law, Code, and the Play of Everyday Practice, Yale University Press.

Coleman, Gabriella (2009). “Code is Speech: Legal Tinkering, Expertise, and Protest among Free and Open Source Software Developers”, 24 *Cultural Anthropology* 420.

Coleman, E. Gabriella and Alex Golub (2008). “Hacker Practice: Moral genres and the cultural articulation of liberalism”, 8 *Anthropological Theory* 255.

Cooter, Robert (1996). “Normative Failure Theory of Law”, 82 *Cornell Law Review* 947.

Cooter, Robert D. (2000). “Three Effects of Social Norms on Law: Expression, Deterrence, and Internalization”, 79 *Oregon Law Review* 1.

Directive 2009/24/EC of 23 April 2009 on the legal protection of computer programs [2009] OJ L111/416.

Disini, Jr., Jesus M. and Janette C (2000). Toral, Annotations on the Electronic Commerce Act and its Implementing Regulations (Philexport 2000).

Dizon, Michael Anthony C. (2011). “Laws and Networks: Legal Pluralism in Information and Communications Technology”, 15 *Journal of Internet Law* 1.

Dizon, Michael Anthony C. (2010). “Participatory democracy and information and communications technology: A legal pluralist perspective”, *European Journal of Law and Technology*, Vol. 1, Issue 3.

Doctorow, Cory (2008). “Amazon reviewers clobber Spore DRM” <http://boingboing.net/2008/09/07/amazon-reviewers-clo.html> accessed 6 December 2012.

Dohrenwend, Bruce P. (1959). “Egoism, Altruism, Anomie, and Fatalism: A Conceptual Analysis of Durkheim’s Types”, 24 *American Sociological Review* 466.

Dommering, Egbert (2006). “Regulating Technology: Code is not Law” in E Dommering and L Asscher (eds), *Coding Regulations: Essays on the Normative Role of Information Technology,* TMC Asser Press.

Downes, Larry (2009). The Laws of Disruption: Harnessing the New Forces that Govern Life and Business, Audible.

Dyson, George (2012). Turing’s Cathedral: The Origins of the Digital Universe, Random House Audio.

Electronic Frontier Foundation, “Computer Fraud And Abuse Act Reform” <https://www.eff.org/issues/cfaa> accessed 4 March 2013.

European Commission, “Communication on a comprehensive approach on personal data protection in the European Union” COM(2010) 609 final.

European Commission, “Communication on a Digital Agenda for Europe” COM(2010) 245 final/2.

Floridi, Luciano (2012). “Norms as Informational Agents and the Problem of their Design”, *SCRIPT Conference: Law and Transformation*, Edinburgh, June 2012.

Free Software Foundation, “What is free software?” <http://www.gnu.org/philosophy/free-sw.html> accessed 5 December 2012.

Galligan, D.J. (2007). *Law in Modern Society,* Oxford University Press.

Geertz, Clifford (1983). Local Knowledge: Further Essays in Interpretative Anthropology, Basic Books, Inc.

Gibbs, Jack P. (1981). Norms, Deviance, and Social Control: Conceptual Matters, Elsevier.

Gibbs, Jack P. (1965). “Norms: The Problem of Definition and Classification”, 70 *American Journal of Sociology* 586.

Gibbs, Jack P. (1966). “The Sociology of Law and Normative Phenomena”, 31 *American Sociological Review* 315.

Giddens, Anthony (2009). *Sociology,* 6th edn, Polity Press.

Giddens, Anthony (1984). The Constitution of Society: Outline of the Theory of Structuration, Polity Press.

Griffiths, Anne (2002). “Legal Pluralism” in R Banakar and M Travers (eds), *An Introduction to Law and Social Theory*, Hart.

Griffiths, John (1986). “What is Legal Pluralism?”, 24 *Journal of Legal Pluralism & Unofficial Law* 1.

Grossman, Lev (2000). “Attack of the Love Bug”,*TIME* (15 May 2000).

Hafner, Katie and John Markoff (1991). Cyberpunk: Outlaws and Hackers of the Computer Frontier, Corgi Books.

Hammond, Martin L. (2004). “Moore's Law: The First 70 Years”, *Semiconductor International* (1 April 2004).

Hampson, Noah C.N. (2012). “Hacktivism: A New Breed of Protest in a Networked World”, 35 *Boston College International and Comparative Law Review* 511.

Hecter, Michael and Karl-Dieter Opp (eds) (2001). *Social Norms*, Russel Sage Foundation.

Hildebrant, Mireille, “A Vision of Ambient Law” in R. Brownsword and K. Yeung (eds) (2008). *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes,* Hart Publishing.

Himanen, Pekka (2001). The Hacker Ethic and the Spirit of the Information Age, Secker & Warburg.

Hollinger, Richard C. (2001). “Computer Crime” in David Luckenbill and Denis Peck (eds), *Encyclopedia of Crime and Juvenile Delinquency (Vol. II),* Taylor and Francis.

Hollinger, Richard C. (1991). “Hackers: Computer Heroes or Electronic Highwaymen”, 21 *Computers & Society* 6.

Hoppe, Robert (1999). “Policy analysis, science and politics: from ‘speaking truth to power’ to ‘making sense together’”, 26 *Science and Public Policy* 201.

Howard, Philip N. and others (2011). “Opening Closed Regimes: What Was the Role of Social Media During the Arab Spring?” <http://pitpi.org/index.php/2011/09/11/opening-closed-regimes-what-was-the-role-of-social-media-during-the-arab-spring/> accessed 7 December 2012.

Hume, David (1739). *A Treatise of Human Nature*<http://www.gutenberg.org/files/4705/4705-h/4705-h.htm> accessed 7 March 2013.

Hutchinson, Lee (2012). “Ubisoft backtracks on PC DRM, citing customer feedback” Ars Technica <http://arstechnica.com/gaming/2012/09/ubisoft-backtracks-on-pc-drm-citing-customer-feedback/> accessed 6 December 2012.

Intel, “Moore’s Law” <http://download.intel.com/museum/Moores_Law/Printed_Materials/Moores_Law_2pg.pdf> accessed 7 September 2012.

Jasanoff, Sheila (1996). “Beyond Epistemology: Relativism and Engagement in the Politics of Science”, 26 *Social Studies of Science* 393.

Jasanoff, Sheila (1991). “What Judges Should Know About the Sociology of Science”, 32 *Jurimetrics* 345.

Jordan, Tim and Paul Taylor (2008). “A sociology of hackers”, 46 *The Sociological Review* 757, 774-775.

Karagiannopoulos, Vasileios (2012). “China and the Internet: Expanding on Lessig’s Regulation Nightmares”, 9:2 *SCRIPTed* 150 <http://script-ed.org/?p=478> accessed 2 October 2012.

Latour, Bruno (2010). The Making of Law: An Ethnography of the Conseil D’Etat (Polity Press 2010).

Leenes, Ronald (2011). “Framing Techno-Regulation: An Exploration of State and Non-state Regulation by Technology”, 5 *Legisprudence* 143.

Lemley, Mark A. and David McGowan (1998). “Legal Implications of Network Economic Effects”, 86 *California Law Review* 479.

Lessig, Lawrence (2006). *Code: version 2.0,* Basic Books.

Lessig, Lawrence (1995). “Social Meaning and Social Norms”, 144 *University of Pennsylvania Law Review* 2 181.

Levy, Steven (2010). *Hackers: Heroes of the Computer Revolution*, O’Reilly Media, Inc.

Ludlow, Peter (2010). “Wikileaks and Hacktivist Culture”,*The Nation* (New York, 4 October 2010).

MacKenzie, Donald and Taylor Spears “‘The Formula That Killed Wall Street’?: The Gaussian Copula and the Material Cultures of Modelling” <http://www.sps.ed.ac.uk/__data/assets/pdf_file/0003/84243/Gaussian14.pdf> accessed 7 December 2012.

McAdams, Richard H., and Eric B. Rasmusen (2007).“Norms and the Law” in A Polinsky and S Shavell (eds), *Handbook of Law and Economics, Volume 2*, Elsevier.

McCullagh, Declan and Milana Homsi (2005). “Leave DRM Alone: A Survey of Legislative Proposals Relating to Digital Rights Management Technology and Their Problems”, *Michigan State Law Review* 317.

Merry, Sally Engle (1988). “Legal Pluralism”, 22 *Law & Society Review* 869.

Michaels, Ralf (2005). “The Re-*State*-Ment of Non-State Law: The State, Choice of Law, and the Challenge from Global Legal Pluralism”, 51 *The Wayne Law Review* 1209.

Mifsud Bonnici, Jeanne Pia (2007). *Self-Regulation in Cyberspace*, TMC Asser Press.

Mitnick, Kevin and William L. Simon (2011). Ghost in the Wires: My Adventures as the World’s Most Wanted Hacker, Blackstone Audio.

Morgan, Bronwen and Karen Yeung (2007). *An Introduction to Law and Regulation: Text and Materials*, Cambridge University Press 2007.

Morozov, Evgeny (2011a). “Facebook and Twitter are just places revolutionaries go”, *The Guardian* (7 March 2011) <http://www.guardian.co.uk/commentisfree/2011/mar/07/facebook-twitter-revolutionaries-cyber-utopians> accessed 5 March 2013.

Morozov, Evgeny (2011b). The Net Delusion: How Not to Liberate the World, Penguin Books.

Morris, Richard T. (1956). “A Typology of Norms”, 21 *American Sociological Review* 610.

Murray, Andrew D. (2007). The Regulation of Cyberspace: Control in the Online Environment, Routledge-Cavendish.

Murray, Andrew and Colin Scott (2002). “Controlling the New Media: Hybrid Responses to New Forms of Power”, 65 *The Modern Law Review* 491.

Olivenbaum, Joseph M. (1996). “<CTRL><ALT><DEL>: Rethinking Federal Computer Crime Legislation”, 27 *Seton Hall Law Review* 574.

Open Source Initiative, “The Open Source Definition” <http://opensource.org/osd> accessed 5 December 2012.

Opp, K.D. (2001). “Norms” in N Smelser and P Baltes (eds), *International Encyclopedia of the Social & Behavioral Sciences*, Elsevier.

Pabico, Alecks P. and Yvonne T. Chua (2001). “Cyberspace has become the playground of high-tech criminals”<http://pcij.org/imag/Online/cybercrimes.html> accessed 2 October 2012.

Pertierra, Raul (2010). “The Anthropology of New Media in the Philippines”, Institute of Philippine Culture 2010.

Philippine Electronic Commerce Act, adopted 14 June 2000.

Pinch, Trevor J. and Wiebe E. Bijker (1984). “The Social Construction of Facts and Artefacts: or How the Sociology of Science and the Sociology of Technology might Benefit Each Other” 14 *Social Studies of Science* 399.

Polanyi, Michael (2000). “The Republic of Science: Its Political and Economic Theory”, 38 *Minerva* 1.

Posner, Eric A. (2000). *Law and Social Norms,*Harvard University Press.

Posner, Richard A. (1997). “Social Norms and the Law: An Economic Approach”, 87 *AEA Papers and Proceedings* 365.

Reindenberg, Joel R. (1997). “Lex Informatica: The Formulation of Information Policy Rules Through Technology”, 76 *Texas Law Review* 553.

Riesenfeld, Dana (2010). *The Rei(g)n of “Rule”*, Ontos verlag.

Rogers, Tomas and Andrew Szamosszegi (1986). “Fair use in the U.S. Economy: Economic Contribution of Industries Relying on Fair Use”, Computer & Communications Industry Association.

Ruby, Jane E. (1986). “The Origins of Scientific ‘Law’”, 47 *Journal of the History of Ideas* 341.

Salmon, Felix (2009). “Recipe for Disaster: The Formula That Killed Wall Street”, *Wired Magazine* Issue 17.03.

Savarimuthu, Bastin Tony Roy and Stephen Cranefield (2011). “Norm creation, spreading and emergence: A survey of simulation models of norms in multi-agent systems”, 7 *Multiagent and Grid Systems* 21.

Schumpeter, Joseph A. (1962). “The Process of Creative Disruption” in *Capitalism, Socialism and Democracy*, Harper Torchbooks.

Skibbel, Reid (2003). “Cybercrimes & Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act”, 18 *Berkeley Technology Law Review* 909.

Sprinkel, Shannon C. (2001). “Global Internet Regulation: The Residual Effects of the ‘ILOVEYOU’ Computer Virus and the Draft Convention on Cyber-Crime”, 25 *Suffolk Transnational Law Review* 491.

Stepanova, Ekaterina (2012). “The Role of Information Communication Technologies in the ‘Arab Spring’” <http://www.gwu.edu/~ieresgwu/assets/docs/ponars/pepm_159.pdf> accessed 7 December 2012.

Sterling, Bruce (1992). *The Hacker Crackdown*, Bantam Books.

Sunstein, Cass R. (1996). “Social Norms and Social Roles”, 96 *Columbia Law Review* 903.

The Mentor, “The Hacker Manifesto” <http://www.phrack.org/issues.html?issue=7&id=3> accessed 4 December 2012.

Therborn, Goran (2002). “Back to Norms! On the Scope and Dynamics of Norms and Normative Action”, 50 *Current Sociology* 863.

Thompson, Clive (2005). “The BitTorrent Effect”,*Wired Magazine* Issue 13.01.

Turkle, Sherry (2005). *The Second Self: Computers and the Human Spirit* (Twentieth anniversary edition), the MIT Press.

Van der Hof, Simone and Kees Stuurman (2006). “Code as Law” in BJ Koops and others (eds), *Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-Liners*, TMC Asser Press.

Von Benda-Beckmann, Franz (2002). “Who’s Afraid of Legal Pluralism”, 47 *Journal of Legal Pluralism* 37.

Von Benda-Beckmann, Franz and Keebet von Benda-Beckmann (2006). “The Dynamics of Change and Continuity in Plural Legal Orders”, 53-54 *Journal of Legal Pluralism* 1, 14.

Williams, Sam (2002). Free As In Freedom: Richard Stallman’s Crusade for Free Software, O'Reilly.

WIPO Copyright Treaty, adopted on 20 December 1996.

World Performance and Phonograms Treaty, adopted on 20 December 1996.