MEDIA@LSE
Department of Media and Communications

MEDIA@LSE Working Paper Series

Editors: Bart Cammaerts, Nick Anstead and Ruth Garland

No. 31
Peer-To-Peer Law:

Distribution as a Design Principle for Law

Mélanie Dulong de Rosnay

Other papers of the series are available online here:
http://www.lse.ac.uk/media@lse/research/mediaWorkingPapers/home.aspx

Mélanie Dulong de Rosnay (melanie.dulong@cnrs.fr) is a permanent researcher at the French National Centre for Scientific Research (CNRS). She heads the Information and Commons Governance research group of the Institute for Communication Sciences (CNRS / Paris-Sorbonne / UPMC). She is a visiting Fellow at the London School of Economics and Political Science Department of Media and Communications (2013-15). A graduate in political sciences and a PhD in law, associated researcher at CERSA (CNRS University Paris 2), where she was Creative Commons France legal lead between 2003 and 2013, she has been research fellow at the Berkman Center for Internet & Society of Harvard Law School (2007-08) and Science Commons and at the Institute for Information Law of the University of Amsterdam (2009-10) prior to joining CNRS in 2010. In 2011 she co-founded in Communia, an international association on the digital public domain, which she currently chairs and represents at the World Intellectual Property Organization. She is regularly teaching copyright law.

Her publications are available at: http://www.iscc.cnrs.fr/spip.php?article1558

Published by Media@LSE, London School of Economics and Political Science ("LSE"), Houghton Street, London WC2A 2AE. The LSE is a School of the University of London. It is a Charity and is incorporated in England as a company limited by guarantee under the Companies Act (Reg number 70527).

ISSN 1474-1938/1946

Peer-To-Peer Law:

Distribution as a Design Principle for Law

Mélanie Dulong de Rosnay

ABSTRACT

Instead of applying law to peer-to-peer in order to control networks, I propose to apply peer-to-peer to the law to transform it. The western liberal conception of law is based on the legal category of the individual. This legal theoretical conception does not adequately take into account the concept of communities of peers, defined as non-stabilised, evolving, or non formalized groups sharing a common interest or an ad hoc production purpose, from local communities (e.g. those using a commons-based governed fishery) to online communities (e.g. the users of a platform) which do not have a legal statute as an individually identifiable entity.

Legal thinking can be influenced by architecture design principles based on decentralisation. Peer-to-peer architectures, for example distributed storage and wireless mesh network, disrupt the application of positive law and question central legal notions of liability, control, ownership and responsibility. I call for a transformation of legal thinking and logic and a theoretical break from envisioning the individual person as unique point of reference of the regulatory system composed by positive law and policies targeting individuals. Network theorists have already been conceptualising the agency of collectives, and commoners have been developing legal hacks to organise collective property. Beyond an individualised law trying to control distributed Information and Communication Technologies, peer-to-peer ways to think and design the law require to design collective rights and legal persons. Challenging liberal legalism design grounded in individualism requires to integrate peer-to-peer as a design principle for the law, towards the recognition of collectives as subjects of rights and duties, and the distribution of the law itself.

INTRODUCTION

The relation between peer-to-peer and the law is often analysed from the angle of file-sharing regulation. Peer-to-peer is seen as a disruptive technology of distribution, requiring the law to adapt itself in order to control a new type of activity. A polarised discourse leads copyright law to be extended to prevent file-sharing from disrupting existing business models based on a strong enforcement of copyright; the alternative policy proposal to adapt copyright law to peer-to-peer file sharing technologies is to introduce limitations and exceptions to exclusive rights in order to preserve user's rights. This relation between law and technology which assumes that the law has to be adapted to take into account new formats of cultural practices, either to forbid them or to legalise them, has been observed for previous changes of peer reproduction and distribution medium; what Walter Benjamin called mechanical reproduction. Both ways to adapt the law to the technology mean that the law is trying to control the technology, either negatively by outlawing certain behaviors, or positively by recognising them. And eventually, after a period of conflict between established rights-holders of the old technology disrupted by a new technology (radio, videocassette recorder, etc), the law reconfigures itself by creating an exception to exclusive rights to open up the system and host the new reproduction technology. With peer-to-peer distribution, new forms of compensation can be considered. Propositions of creative contribution (Aigrain, 2012) favor the concept of peers contributing to the creative process in a redistributed manner, instead of relying on the centralisation of a collecting society to collect and share remuneration based on usage of cultural works.

This article positions itself beyond the tension between copyright enforcement to preserve business models *vs* users' rights required to enjoy the opportunities provided by the disruptive technology for access to knowledge. Instead of *applying law to peer-to-peer* in order to control networks, I propose by *applying peer-to-peer to the law* to consider another angle of the relation between law and technology and to introduce the argument of the distribution of the law itself. Peer-to-peer technologies disrupting established economic models and legal categories could also inspire an evolution of the law as a regulatory system in order to integrate some of their technical features. This will lead to another kind of relationship between law and technology: after the control of the technology by the law which absorbs the new technology by expansion of its application scope, and in addition to the scholarship on regulation by code or of code (Lessig, 2006; Brown & Marsden, 2013), the law can try to integrate the technology. It might do so by reconfiguring its internal operating system and shuffling the categories a bit more, instead of simply inflating them by adding an exception to the existing system.

My starting point is that the western conception of law is based on the legal category of the individual to which rights and duties are allocated in balance with others'. The fictional notion of the individual person includes the citizen, the user, matching the notion of a real person, but also all individually identifiable actors which have been allocated a legal status as a single entity: corporations, non-profits, nation states, all kinds of organisations. But this legal theoretical conception does not adequately take into account the concept of communities of peers, defined as non-stabilised, evolving, or non formalized groups sharing a common interest or an ad hoc production purpose, from local communities (e.g. those using a commons-based governed fishery, Ostrom, 1990) to online communities (e.g. the users of a platform) which do not have a legal statute as an individually identifiable legal entity.

Law, as a technology of regulation, can be disrupted by peer-to-peer, not only in order to evolve to apply to new objects, but also in the sense that legal thinking can be influenced by its architecture design principles based on decentralisation. Peer-to-peer networks, source of peer production of content or services, as disruptive online technologies, reconfigure legal categories' frontiers and assumptions. Collective mechanisms of governance and ownership by peers are identified in the traditions of the natural commons (Ostrom, 1990), of social movements and for the recognition of local communities' rights. They offer not only a political alternative, but also a theoretical break from envisioning the individual person as unique point of reference of the regulatory system composed by positive law and policies targeting individuals, towards the recognition of collectives as subjects of rights.

In this article, I consider law as a technology raising policy questions. I will first describe how the concept of distributed architectures, the technical underlying feature of peer-to-peer systems as opposed to centralised design of client-server communication, is disrupting the application of positive law. Legal disruption of copyright by peer-to-peer file-sharing services has been studied extensively, but other applications based on distributed technology also question liability, control, ownership and responsibility. I chose to focus on two specific instances of peer production to develop my argumentation: peer production of storage and peer production of connectivity.

Distributed storage and wireless mesh networks will be addressed in section 1. In section 2, I call for a transformation of legal thinking and logic. Instead of relying only on the concept of the individual, I am questioning whether the law could integrate the architectural features of distribution from the inside of its categories in order to try to better regulate distributed technologies. Peer-to-peer ways to think and design the law are already being developed by the political movement of the commons and by network theorists. I consider

in section 3 such attempts of designing collective rights or collective persons beyond both a mere individualised law and Information and Communication Technologies. A peer-to-peer law also relates to political theory questions of plural persons and the agency of collectives. But in order to really challenge liberal legalism design grounded around individualism, I conclude in section 4 with the need to develop metaphors and social imaginaries (Mansell, 2012) to conceptualise empty spaces (Milun, 2011) which are more difficult to envision, and contribute to the definition of distributed forms of ownership, responsibility or liability as examples of integration of peer-to-peer as a design principle for the law.

THE IMPACT OF DISTRIBUTED ARCHITECTURES ON LEGAL LIABILITY

The architectural design of peer-to-peer challenges legal reasoning and the usual application of concepts such as property, or the assignment of responsibility, because files and actions are fragmented, distributed between nodes hosted by peers, rather than directly attributable to individuals. Peer-to-peer networks are relying on decentralised architectures as opposed to direct relations between a server and clients (Dulong de Rosnay, 2013). Similarly, peer-production is a system of production which differ from the centralised, liberal model of the firm in the sense that it functions around collaborative dynamics with a non hierarchical, self-organising structure and if ownership is also distributed, it will be commons-based peer-production (Benkler, 2006).

Many technologies are designed according to distributed, decentralized principles. Distributed architectures are considered as social technologies, in the sense that they allow peer production and reach a common goal or individual needs through coordination of shared resources[1]. Instead of bi-directional client-server relations, all peers possess and demand the resource, and enter into a spontaneous collaboration without need for central coordination (Schollmeier, 2001), resulting in decentralised resources distributed among unpredictable IP addresses (Shirky 2000). Peer-to-peer designates 'any networking technology where crucial responsibility lies at the end-points' (Oram 2004).

From a strictly technological point of view, it should be noted here that pure decentralised peer-to-peer does not exist: applications are relying on hybrid models, with a small dose of centrality, as they are sometimes structured around supernodes which re-create a degree of centralisation. These implementation features are important to make the services more efficient and above all stable (Elkin-Koren, 2006).

[1] The following presentation of distributed architectures draws from and builds upon the introduction of Musiani, 2013.

However, for the sake of theoretical reasoning I will ignore these implementation considerations and focus on the distributed aspect of peer-to-peer architectures, how it may impact on the application of the law (section 1) and how it may influence the design of the law (section 2). Indeed, in order to improve quality of service, resource optimisation and resilience to network problems such as connectivity interruption, files are fragmented among peers. With the Bittorent protocol, for example, only the final peer reconstructs the file (Cohen, 2003).

This architectural configuration based on resource sharing has an impact on the localisation of data and exchange. Forces of decentralisation and autonomy characterise distributed services, as each node can be client and server and no node controls the other. Localisation and control are useful conceptual notions at the foundation of legal reasoning and therefore the allocation and attribution of rights such as responsibility or ownership. By looking more precisely at two distributed technologies, I intend to demonstrate how their design questions the application of traditional legal regulation which is based on legal fictions of *individualisable* and individualised actions, objects and persons.

Distributed Storage

An example of peer-to-peer technology disrupting the legal frameword is Wuala (a case study analysed by Musiani, 2013 and 2014). Wuala, initially developed by the Swiss Federal Institute of Technology (ETH) in Zürich, is a distributed storage service[2], like Dropbox, except that hosting of the files to be backed up is not centralised on the (single or multiple units of individually identifiable cloud) servers of the company, but rather distributed among the hard drives of users of the service which are linked to each other in a distributed network architecture. In order to ensure a better quality of service, it also features more traditional cloud data server modalities of hosting (Mowbray, 2009). But for the sake of argumentation, I choose to consider only the peer-to-peer portion of the service which could theoretically be used on a standalone basis without additional storage in the application centralised cloud server. Even if it is not the best product from a marketing or usability point of view, the distributed part of the service is the socio-technical arrangement and the legal tendency I want to observe.

When uploaded to Wuala, data is fragmented, locally encrypted on the machine of the user and made redundant, in order to ensure availability for download even when not all the

[2] See: https://www.wuala.com/en/learn/technology

peers offering their internal disk for shared storage are online at the moment the user who uploaded the file wants to access it again (in the same way it is necessary to have at least one 'seeder' to download a torrent). Therefore, if no file is stored entirely, it is questionable whether contributory or induced liability would be triggered at all, if a file contains illegal content. Unlike Bittorent, peers do not know what they are hosting as the files, after being fragmented, are encrypted.

Besides, the service can't technically monitor[3] what is being uploaded because of the distribution of the process. External entities (majors, police) can't proceed to the surveillance of the files either. Indeed, at no time are files existing in a reconstituted format, making them readable and perceptible to the senses, outside of the machine of the first peer who uploads it bits by bits and downloads it back fragment by fragment.

Therefore, it is legitimate to question, as Musiani does (2013: 221), whether users could be held liable for helping someone to reproduce and access an infringing file. It seems impossible to assign intention, awareness or even to detect guilt in the mere transient action of hosting fragments, as neither the peers nor the service developers have the technical means to know what they are hosting. Circulating in sealed envelopes fragmented among many hard drives, stored content can contain holiday pictures for back-up purposes, copyrighted books, personal data, revenge porn or harmful content. And none of the nodes is essential since redundancy allows the use of other ways if one is missing or offline, diminishing the responsibility even more.

A second version of Wuala added a part of centralisation to improve the service, but it is likely that in a purely distributed configuration, neither the peers nor the service could know what is hosted, except if managing to break the encryption which is not possible in the current state of the art. Therefore, no procedure of notice-and-take down[4] or limitation of the liability of the Internet Service Provider could apply as the reconstituted content will never be visible nor made public: if illegal content would remain unnoticed, no-one could notify anyone or remove any content. If the data remains fragmented and private, even forcing the service to reveal the identity of the registered users would not help the justice as it would not inform of the lawful or unlawful nature of their activity.

[3] There are similar instances of technical impossibility to reveal the content for technology providers (unlock an encrypted iPhone) but the ability and legal responsibility to give data, for instance in case of warrant, still applies to Apple cloud centralised architecture :
http://www.washingtonpost.com/business/technology/2014/09/17/2612af58-3ed2-11e4-b03f-de718edeb92f_story.html

[4] As requested by the Digital Millennium Copyright Act 1998 and the Electronic Commerce Directive 2000.

The only pressure public authorities could place on a service which may potentially host content infringing the law could be intimidation (Lavabit encrypted email service provider decided to close the service rather than giving its encryption keys[5], but Wuala does not know the password of its users). Another more radical option is outlawing distributed services as a technology. This regulatory move would have a chilling effect[6] and prevent legal activities, in the same way peer-to-peer filesharing protocols can be used both to download free software, public domain works or unauthorised content. But unlike Dropbox (which is hosting the files and does not allow the storing of certain files[7] which might be copyrighted and the service incidentally used as a filesharing platform), a distributed Wuala would not be able to control what files or even file formats are being uploaded and fragmented. Indeed, the encryption is performed locally on the user's machine before the fragments get duplicated and hosted on the hard drives of other peers.

The PirateBay has an index of links to available torrents, which can be legally problematic in some jurisdictions, and offer a means of technical control through an order of blocking to be sent to the Internet Service Provider on the request of the government or the major companies. The level of decentralisation matters and if only the delivery is distributed but the production remains centralised, the service will be vulnerable. But as there is no such centralised information on the torrents of the files for Wuala, which acts as a distributed private storage cloud, there is no such option to remove or block the page with links to the content, or to know which fragment belongs to which user.

Musiani (2013) speaks about a 'shared techno-legal responsibility'. Crowd-sourced infringement management or distributed policing can work in the case of harmful content (e.g. child porn) disseminated on Facebook because a user can report the content in one click. Diaspora distributed social network foundation is contacting the administrators of nodes hosting Isis propaganda[8]. Copyrighted images on Wikipedia can effectively be removed by patrols of editors who want to protect the commons-based peer-production from legal liability. But private policing without accountability presents risks of discrimination and I do not think self-regulation by the users could ensure the legality of the content hosted, if only the uploader is aware of the content of the file. Also, the disclaimer of liability contained in the terms of service of the application would probably not be helpful against a legal attack. Ethical considerations such as community monitoring, or

[5] See: http://www.theguardian.com/commentisfree/2014/may/20/why-did-lavabit-shut-down-snowden-email

[6] See: https://www.chillingeffects.org/

[7] See: http://www.extremetech.com/computing/179495-how-dropbox-knows-youre-a-dirty-pirate-and-why-you-shouldnt-use-cloud-storage-to-share-copyrighted-files

[8] See: http://www.theguardian.com/technology/2014/aug/21/islamic-state-isis-social-media-diaspora-twitter-clampdown

commitment to host only lawful content, can be useful to self-regulate and police a service to ensure its sustainability as a commons, based on Ostrom's Institutional Design Principle #4: 'Effective monitoring by monitors who are part of or accountable to the appropriators' and its complement #5: 'A scale of graduated sanctions for resource appropriators who violate community rules' (Ostrom, 1990). But more pragmatically in the case of a distributed service such as Wuala, if no infraction can be detected, it seems very unlikely that such a feeling of community responsibility could be developed.

Similarly, I seriously doubt that liability could be assigned to the service provider (except in the case peer-to-peer technologies would be outlawed altogether with their developers), nor to some individual nodes (legal regulation did not reach that stage of control yet and intermediary law is protecting them). It seems difficult to allocate individual responsibility to individuals who share their computing resources with unknown peers to reproduce and communicate content of unknown nature. Judicial proceedings for negligence to secure one's wireless connection have been implemented both in France with the three strike law[9] and in the US with police raids. However, the identification of the IP address of the device, which is dynamically changing over time and can be changed or spoofed, is not sufficient proof to identify a person.

Wireless Mesh Networks

Mesh wireless technology (Jun, et al., 2003; Chen et al., 2006) makes it even more difficult to assign liability to an IP address, as IP can be shared among even more peers using the network than with conventional WiFi. To increase security, these services can also be used in conjunction with applications for encryption and anonymisation, such as Tor[10], The Onion Router distributed browser ensuring the routing of communications through a network of nodes hosted by peers, masking the IP. The implication of such architectures is anonymisation and privacy-by-design (Langheinrich, 2001). Both online privacy for activists in undemocratic countries or journalists who need to protect their sources and the dissimulation of illegal activities are users of Tor. Anonymisation of the source should be well ensured if it is hard to find the source or the destination of the content (Li, 2007).

Wireless mesh networks, which can be used by wireless local communities (Antoniadis et al., 2008 and 2009), municipalities or hackers, apply the same principle of routing the communications between nodes (laptops, phones or other wireless devices). The network

[9] French Hadopi or Creation and Internet law (see Lovejoy, 2011 and Jondet 2010) tried to hold users liable for not securing their internet connection and allowing other users to perform infringing activities on their wifi. It was introduced in 2009 and until its revocation in 2013, only one user had its connection suspended.

[10] https://www.torproject.org

can be connected to the internet or not, and communication can be organised either around a central server or in a decentralised way, as considered in this paper. One node will only transmit to the next node. In order to avoid secondary liability for actions led by other users of one's internet connection, in the jurisdictions where it exists, it is possible to use a Virtual Private Network (VPN)[11]. There is community governance and self-regulation as many networks offering free service of transit commit to certain principles organising the relation between nodes[12]. However, these agreements intend to regulate *tort* regarding the quality of service, not the potential infringing activities committed on the network. Applying the law of Internet Service Providers (ISPs)[13] to mesh node owners, nodes cannot be held liable for content infringement. Mesh nodes would be 'common carriers' or 'mere conduits': simply relaying data, and thus benefit from a legal immunity (Hatcher, 2007). Law enforcement would be more difficult for distributed community-based networks formed by many individuals than for municipalities or universities who would demonstrate centralisation at the level of the ownership of the network, while peer-to-peer mesh networks seem 'copyright resistant' (von Lohmann, 2004). Depending on the legal status of the mesh network, the regime of ISP liability may or may not apply: in the case of an association with a board and legal representatives for the community mesh network, or if a node is held by an institution, it could be held liable for the traffic, but in the case of a distributed architecture without designated responsible persons or contractual relationship, it seems more difficult to enforce the law (Guadamuz, 2011; Dulong de Rosnay, 2013; Giovanella, 2014). This is all the more pertinent when creating a node does not require registration and the number of nodes is unknown, and in the case of encrypted mesh network, forming a local darknet. Like for distributed storage, allocating liability to individual nodes of the mesh is difficult because the connectivity is made possible by a distributed network of devices. Peers hosting Tor relays or mesh network nodes should not be held liable as they are not the ones using the service to perform an illegal activity. Intermediaries in general should not be held liable:

> Holding intermediaries liable for the content disseminated or created by their users severely undermines the enjoyment of the right to freedom of opinion and expression, because it leads to self-protective and over-broad private censorship, often without transparency and the due process of the law. (La Rue, 2011: 12).

[11] See: https://en.wikipedia.org/wiki/Freifunk

[12] See: http://www.picopeer.net/PPA-en.html

[13] Directive 2000/31/EC of 8 June 2000 on Electronic Commerce, OJ 2000 L 178/1, Article 12; US copyright law 17 USC 512(a).

FOR A TRANSFORMATION OF LEGAL THINKING

Lobbying to prohibit peer-to-peer file sharing or peer-to-peer based technologies of anonymity, storage, browsing or access follows a traditional model of legal regulation, which aims to control technology and safeguard the supremacy of legal rules which were developed before the emergence of the new technical environment. However, this position, instead of transposing legal values and general principles to the digital age, leads to constraining it beyond the initial regulatory objective of preventing infringement, by controlling also legitimate activities which were previously unregulated. Legal doctrine showed the extension of the scope of copyright and the chilling effect on users' rights and socio-cultural practices of creation. The law has not been updated yet to scale to the technology. There has not been any change of legal paradigm to integrate transformations caused by digital technologies and especially peer production with unidentifiable networks of peers instead of legally identifiable persons. Law can also interact with technology in a different way by trying to integrate some of its features in order to maybe regulate it better.

One way to think about the relationship between law and peer-to-peer technology is to wonder if the law needs to be expanded to face a new regulatory challenge. People choose to use and to contribute to services based on distributed architectures for many reasons including to preserve their privacy and escape censorship, but also legal control. The uniqueness of the distributed environment may fade away if the legislator catches up and blocks the ports needed to deploy peer-to-peer architectures. The same attack of 'law of the horse' (Easterbrook, 1996 and the answer by Lessig, 2001) which has been made to cyberlaw could be made to a law of distributed architecture, questioning its singularity and its *raison d'être*. Or, if distributed architectures are unique, we are facing the emergence of new legal categories which will produce new norms. But beyond the fact that these technologies may be used for both legitimate and illegal purposes and that the fragmentation of the services makes it difficult to assign liability, it should be noted that these peer-to-peer services are also part of the social movement of the commons. They foreground peer-production as an alternative to the market-based centralised services exercising control over their users and their data. Even if technical efforts required to set them up as opposed to the ease of installation of their commercial counterpart may prevent their take-off, they participate in emancipation and autonomy through technology, and constitute a valid alternative to the commodification of free labour and the lack of security and privacy of the commercial services.

From a legal perspective, the main difference I want to observe between commercial and peer-to-peer services is that the former services rely on a contractual relation between two

individual entities (the corporation and the user), allowing the allocation of responsibility in case of infringement, while the latter services are not provided by an individual person. They are offered by a mesh of nodes which ensure collectively that the service is possible, each ensuring a fragment of it, which is difficult or impossible to monitor technically and control legally. Distributed architectures are fragmenting data and actions, thus exploding the localised rights model where each object or right can be assigned to one actor. The problem comes from the fact that peer-to-peer architectures aggregate and distribute technically insignificant fragments, while the law allocates rights to individual persons in a bijective relation.

Individual legal entities are the basis of legal reasoning and the subjects of rights. Western legal systems tend to mainly recognise the rights of individuals, to protect private property rights, commercial interests in individuals and personal freedoms. Law assigns rights to individuals (which can be states, corporations or non-profit) benefitting from autonomy and agency. While law is arranging responsibilities, rights, duties, obligations and conditions between moral or physical persons in localised determined jurisdictions, distributed architectures operate with fragmented data and share the process between actors which are neither localised nor stabilised, as they are not necessarily the same peers present all along a given process of data communication.

I claim therefore that the distribution of the actors and the actions requires the rethinking of legal categories, since the notions of *author* of an action, *action* and *content* or *object* are not tangible units any longer, but aggregated, open-ended and evolving fragments. Legal reasoning will question whether distributed services are really of a different nature; whether localisation really matters; whether the association of encryption and fragmentation ensures anonymity or untraceability; how to distinguish the request of an action from the implementation or performance of the action? Regarding the last question, my understanding is that fragmentation of actions between an unfixed network of peers at least blurs responsibilities and at most makes them irrelevant.

Which method of research of the responsible person can be applied if there is no identifiable owner or service provider? Joint liability of all identifiable nodes for the other members of the group who would have performed an offence has not been applied, but the absence of case law does not mean this could not happen. It might be the case that if no entity is found liable, any identifiable entity related to the case would be sentenced. The reconfiguration through cooperation of the notion of individuals forming a collective triggers a deconstruction of legal categories in several domains: copyright, liability, cybercriminality, processing of personal data, but also data security. In case of service failures and data loss, it

is not certain that a warranties disclaimer would be valid when faced with consumer protection legislation. No contractual relationship can be deduced: since users are unknown and unstable, the performance of the service depends on who is connected at what time, but none of the nodes are individually essential. In the absence of a contract and of user identification, it is difficult to assign responsibility in the traditional way. A complex network of users and contractual relationships could be inferred from who is online when, but if peers do not know what package is circulating, and if the package may take a different road when they are not online, all peers could just be irresponsible nodes among others, unaware of the content of the traffic they are collectively facilitating, but neither individually allowing or blocking. The presence or the absence of one peer in the network is irrelevant to the performance of the service, diminishing claims for collective responsibility.

PRECEDENTS, LEGAL HACKS AND ANALOGIES

The law reasons by analogy. It is therefore useful to examine the state of law in similar or comparable areas. Precedents and contributions to a movement of peer-to-peer law can be found in two areas: the commons and network science.

Fragmented Property Rights Over Physical and Digital Commons

The legal framework for ownership and copyright has been able to address peer production with specific governance arrangements for both physical and digital commons.

Elinor Ostrom's bundle of rights opened a new positive space to think about common or shared property (Orsi, 2013). *Res communis*[14] constitute an alternative to exclusivity through individual private property and unregulated open access to *res nullius*[15] thought negatively as inappropriable. Before enclosure of the lands, property was attached to utility, with different usage rights (De Moore 2009) and natural common-pool resources are considered common property with a distributed bundle of rights (access and withdrawal operational rights, management and governance, exclusion, alienation as collective choice rights). This conception is clearly a conceptualisation of fragmented property among different types of users. Orsi also recalls that already in the 19th century, the US doctrine of legal realism on fragmented property introduced doubt on the pre-existing legal categories,

[14] *Res communis*, or common things, cannot be appropriated and can be used by everyone.

[15] *Res nullius*, literally nobody's things, designate the state of things before they are appropriated, while they are not yet the object of rights.

describing property not as an absolute right but as a collection of social relations, rights, duties, obligations and responsibilities[16].

More recently, Italian water distribution has been the theatre of a movement that uses the constitutionalisation of the commons to exclude both privatisation and nationalisation. Stefano Rodotà (2013) is calling for 'a new definition of "citizen"', one that goes beyond 'a set of rights and duties allocated in a statist perspective'. Defining political participation mechanisms still refers to the citizen as an individual in reference to the right of access to the common goods. A more profound legal epistemological turn transposed to distributed architectures studied in the previous section would depart from citizens as individual commoners, to start considering the actions operated by peers as operated by a collective of a different nature rather than the aggregation of individuals. With water as a commons, the epistemological transformation is affecting the nature of the object of rights, the commons, but not the nature of the subject of rights, who remains an individual citizen and does not become a collective, even if she is granted access to rights to a commons which belongs to everyone.

What is thus required is to define rights and duties directly for collectives, instead of granting rights on the collective object to individuals. It really matters for sustainability to consider not only property in terms of access or copyright, but also to address the question of the responsibilities of the collective of commoners to take care, contribute and repair the infrastructure of the common-pool resource to be maintained in case of failure or a security problem. Monitoring the pollution and fixing mistakes as Wikipedia editors is the digital equivalent to the responsibility of caring. But if Wikipedia production is distributed, its technical infrastructure is centralised. Is there an equivalent treatment for an infringement somewhere in the nodes of the collective for a distributed service such as Wuala or informal communities' mesh networks? Maybe the transformation into commons (instead of exclusive property or ownership) through Copyleft[17] licenses applied to copyrightable intangible works and extended to open hardware (Söderberg, 2013) could be used as a framework to extend the legal hack which has been applied to copyright to other rights or legal concepts such as liability or legal person, and distribute them.

Creative Commons licenses organise a private ordering of a bundle of rights in copyright (Elkin-Koren, 2005), segmenting the right of access (equivalent to the Roman category of

[16] See the table of eleven rights by John Commons (1893) in The distribution of Wealth, reproduced by Johnson (2007) cited by Orsi (2013): http://regulation.revues.org/docannexe/image/10471/img-1.png

[17] Copyleft is a copyright licensing scheme requiring derivative works to be licensed under the same terms than the original work, aiming at propagating certain freedoms to downstream users and avoiding private appropriation. See Elkin Koren 2005, Chen 2011, Barron 2014.

usus), reproduction, derivation, commercial exploitation (or *fructus*) and exclusion (or *abusus*), the latter being neutralised by the Share Alike or Copyleft clause. Distributed property, with the legal hack of the copyleft clause, started from the need to maintain distributed production in the commons in order to avoid exclusion and private enclosure (as defined by Boyle, 2003).

But the organisation of shared property relies on the decision of the licensor, an individual person with exclusive control, comforting 'an author-centric individualism' and an 'implicit adoption of liberal legalism: a perspective on the social world that privileges the rights of individuals over the claims of any social group' (Barron, forthcoming). The smallest denominator across the various licenses, a non-commercial verbatim sharing grant, can be interpreted as a concession of rights by the licensor. Exceptions to exclusive rights, fair use or fair dealing secure better collective rights in the sense they are taken out of the bundle of rights available to the original author.

Network Science and the Agency of Collectives

Distributed ownership can be arranged by copyleft private ordering, guaranteeing rights to the collective. But the governance of the usage, even if all aspects of the bundle of rights are well considered, does not solve the question of the provision and the maintenance of the resource, otherwise it will not be produced or nurtured and available in the first place. Therefore, it is necessary to reason in a systemic way and also consider how other rights and duties may be assigned to collectives. Network science provides examples of distributed responsibility or allocation of responsibility to other entities than individuals.

Literature in law and artificial intelligence has been considering rights of non-human electronic agents (Teubner, 2006) and the intentionality of software agents (Sartor, 2009). For electronic contracting, a solution to avoid a vacuum in contract law is

> to combine the quasi-actions of the non-human contract partner with the actions of an individual person or an organization, usually the owner of the non-human, and to attribute contractual acts – meeting of minds, breach of contract, performance – to this socio-technical ensemble, safely hidden behind the screen of the well-acquainted juridical person (Teubner, 2006: 506).

But the reasoning is still based on the singularity of one juridical person. If a non-human cannot be held liable, the manufacturer or the owner could be, which does not translate well for distributed storage or mesh network, if the activity of hosting or providing the access is fragmented and in the absence of centralised ownership or governance of the service by a

company or a non-profit or a municipality with a representative having a singular legal personality. As for manufacturing, these technologies can be easily replicated and re-developed by others, or mirrored and hosted elsewhere, all the more if they are free or open source software.

Current legal rules applicable to distributed platforms and networks, namely, privacy, tort or ownership, have been developed for firms and individuals rather than for distributed communities and fragmented data. There is no legal theoretical framework to take into account hybrid and evolving networked communities. Regulating mesh wireless networks for infringement by fragmenting the liability among identifiable nodes requires establishing trust within a community. Solidary obligation requires the spread of the liability among different members of the network instead of having a single person (the owner or the coordinator) who is held responsible for the entire network. However, as outlined above holding nodes accountable for the traffic of a wireless network is an arbitrary decision which is not sustainable (another, more simple option would be the absence of regulation and policing with the collective tolerance or acceptance of infringements). So, if the traditional approach to allocate responsibilities cannot be applied, should we look for an alternative system to the tort logic which is looking for responsible individuals? Or should the system be re-thought entirely if the traditional notion of liability is not sustainable requiring another model to be developed in order to organize risk and distribute liability? Networks have been envisioned as connected contracts[18] rather than legal categories (Teubner and Collins, 2011), raising the question of where risks are transfered to in this form of cooperation and myriad of complex relations.

One possible approach could be the development of collective insurances, voluntarily paid by the members of a community to cover the possible risk of trial and losses by users, but it is just a coping mechanism reproducing the logic of a single individual or a group of single individuals jointly found liable. Mechanisms of commons-based mutualisation have been developed to redistribute monetary gains of the sale of a music platform[19] according to commons-based governance mechanism. I interpret this as an adaptation of the collective management observed for commercial music and organised by civil collecting societies often with a public monopoly, where part of the sums collected for private copying in some

[18] German Civil Code Bürgerliches Gesetzbuch (BGB) §358 organises connected contracts in consumer law, with good faith in contract. http://www.gesetze-im-internet.de/englisch_bgb/englisch_bgb.html#p1260

[19] Such a commons-based mutualisation model has been implemented in 2007 to share the revenues of the sale of music on the platform Pragmazic, a project of the Musique Libre non profit organisation (dogmazic.net)

- 'we only distribute labels releasing works under open licenses (Creative Commons, Copyleft);
- albums are available for download in CD quality with no DRM, some are also available in CD format;
- 65% of retail price (excluding tax) goes to beneficiaries;
- 17,5% goes to a free music support fund;
- 17,5% goes to the platform'

See: https://web.archive.org/web/20070521101640/http://www.pragmazic.net/bin/accueil.php

countries are dedicated to creation funds managed by the collecting societies. Instead, the remunerations collected from commercial use are to be redistributed whereby a collective decision-making process decides which future projects will be financed with the money collected from past projects. This collective fund could serve to pay for fines and be a sort of commons-based insurance, funded by an entry fee to join the platforms, which would not be free but reserved to members. However, this modality does not take into account the evolving, anarchic nature of the moment when nodes are and are not sharing their connection.

If the malicious intentionality of the collective can be hard to demonstrate for the distributed platforms besides the peer-production of a performant and autonomous service, is the definition of plural persons less problematic? Collective actors and collective conscience have been the subject of many studies. A state will become a collective actor because of its capacity for action, rights and responsibilities (cf. Luhmann, as recalled in Teubner, 2007), but can this self-referring definition be applied to distributed architectures if no node is indispensable to perform an action which cannot be identified or attributed to the guilty person requesting it because of the fragmentation of the data among peers cooperating blindly?

The lack of intentionality of computers is not a barrier to contract formation[20] (Solum, 1992), but in contract law, 'agents are supposed to dispose of a certain decisional autonomy' (Teubner, 2006: 508), which is not the case for the participation in a distributed project where the peers do not review what they participate to help circulating. The answer may lie in the concepts of actants and hybrids as conceptualised by Latour (2004). Teubner (2006: 512) states that '[i]n hybrids, the participating individual or collective actors are not acting for themselves but are acting for the hybrid as an emerging unit, the association between human and non-humans'. So are Wuala and mesh networks hybrids? If they don't know what they are carrying, there is no a common will or common action, so they do not form an association.

Lindahl (2013) has been looking for 'a theory of law in the first-person plural': the definition of the 'we' of a cyber-community can be found in the Declaration of Independence of the Cyberspace (Barlow, 1996), which is 'potentially everyone; not, however, as an aggregation of individuals but rather as a whole, as a collective that acts jointly'. This relies on the distinction operated by Margaret Gilbert between 'we, each' and 'we, together', with opposed functions as 'aggregative' vs 'integrative' in a joint collective action. She refers with the latter

[20] Section 14 of the US Uniform Electronic Transactions Act

to bird watching or making music. Can the joint provision and usage of distributed storage or connectivity be found under the same banner? According to her, this plural subject can be found when 'One is willing to be the member of a plural subject if one is willing, at least in relation to certain conditions, to put one's own will into a “pool of wills” dedicated, as one, to a single goal (or whatever it is that the pool is dedicated to)' (Gilbert, 1996) and group intention can be found when several persons are 'jointly committed to intending as a body to do A' (Gilbert, 2000: 22), therefore the peer-production on distributed platforms could be considered as that action. But if there seem to be a plural subject, a joint collective action and group intention, does it automatically lead to collective and distributed responsibility?

The concept of collective responsibility has been discussed in relations to horrors committed during wars (Smiley, 2011: np):

> Does it makes sense to distribute collective responsibility in general? Is it appropriate to hold individual group members morally responsible for harm that other group members caused? that the group itself caused? that the group as a whole failed to prevent? [...] Only particular kinds of groups are capable of acting and intending collectively and [...] are capable of being collectively responsible for harm.

Nations and corporations, the first group to which collective intention and responsibility can be recognised according to Smiley, have a single representative legal person, thus a centralised decision-making body. This doesn't apply to distributed storage and community mesh networks to the extend their governance is also distributed and not top-down structured around a legal person (which will be the case for mesh network provided by a municipality).

Smiley (2011) continues with the question of collective responsibility for past generations with an interesting hypothesis: the US does not recognize slavery as genocide and does not pay any reparations as a liberal individualistic society, while Germany has paid reparations as a State to other States for WWI and to the Jewish people for WWII. Thus, could the liberal individualism conception which lays deep inside of legal paradigm prevent the conceptualisation of collective responsibility?

The second group with collective intention and responsibility in Smiley’s analysis are social movements where members have a collective interest. Collective intentionality can be found in such subjects lacking of legal personality: social movements share a political agenda, but they lack a shared sense of rights or duties. Therefore, individual members will be prosecuted by the state in order to try to stop the movement, with all the unfairness which may derive from that for the ones who get caught.

When joining a distributed project like Wuala or hosting a Tor node to facilitate anonymous connection, contributing participants have no way of knowing whether their fragmented contribution to the network will help political dissident, a cybercriminal, a privacy-concerned individual or someone downloading music. Therefore, it is questionable whether joint commitment or responsibility or contract may be applicable and helpful notions in the quest of distributed legal persons, rights or duties.

LOOKING FOR METAPHORS FOR A DISTRIBUTED LAW

In the same way the information society is grounded in social imaginaries (Mansell, 2012), law needs to develop metaphors and narratives to be able to conceptualise what may be unthinkable. The recognition and the protection of the commons is difficult because they are empty spaces lacking a definition (Milun, 2011). The collective is conceptualised in other disciplines, where complexity has been applied[21]. It is possible to hack the law in order to make existing categories fit a new purpose, for example copyleft against copyright enclosure, or *throuple* in the US, one marriage and an additional contract to bind the couple with the third person and give a legal protective status to a polyamorous relation of three persons as close as possible to marriage. But it is still difficult to apply the concept of a collective directly into law.

It is not surprising that the commons are invisible spaces which Western conceptions of law have a hard time dealing with. The material foundations of legal norms, such as the concepts of territory and exclusive property are being challenged by the global commons; international law is failing to protect against enclosure (Milun, 2011). In additon to this, beyond peer-to-peer filesharing, international public law is failing to protect global commons which are being invaded by technological innovations: the sea is depleted by industrial fisheries, space is polluted by satellite garbage, genetic material and biodiversity are privatised by patenting. These commons are treated as *res nullius* that belong to no-one rather than *res communes* which belongs to everyone (Milum, 2011). In the realm of copyright, the notion of public domain is hard to conceptualise as a positive space with rights and only Chile has a definition of the public domain in positive law (Dusollier, 2011). Relating to the reform on the governance of water in Italy, the action transforming a private good into a common good is legally impossible because the neoliberal order is embedded in and supported by the legal system:

[21] See the multitude of Deleuze and Guattari, or the collective intelligence of Pierre Levy.

> The basic problem is that the neoliberal political order – and particularly the system of law – favors private property rights and the corporate sector. (…) If you are a municipality and want to sell your water company, you will find it very easy from a legal point of view. But there are no laws in the Italian legal order that shows you how to go the other way around. (Mattei, 2013: 23)

CONCLUSION

The western legal system is grounded on the individual (private or public) person, while there is a need for cultural change from an individualistic neoliberal paradigm to recognise community rights and duties and collective persons as opposed as individual persons. Indeed, as argued in this paper, applicable law and legal theories are not capable of addressing commons-based distributed collective endeavours where actions, data and persons are fragmented. The fall of the individual, or of the individualisable person as a unique, centralised point of reference, seems to be the only solution to organise the rise of the assignment of legal personhood, and therefore rights and duties, to such communities. To accommodate this evolution of legal regulation and address socially valuable forms of distributed peer-production, transformation is needed at the level of the State and its positive law, both at a community- (the movement of the commons and its self-governance rules) and a market-level (crowd-sourcing and the insufficient regulation of services like Über or Airbnb). To borrow from Wielsch, 'Don't occupy the system, occupy the law!' (Steinbeis, 2012).

Still, there are more examples of collective thinking in the law. It would be useful to consider how non-Western legal orders consider the concept of collective *vs* individual. The *Buen Vivir* movement in Latin-America (cf. Gudynas, 2011) constitutes an alternative paradigm to capitalism's individual private ownnership rights, instead foregrounding collective rights of nature, culture and communities[22]. There are also some collective rights enacted in the second and third generation of human rights, but they are in the end not assigned to collectives, but to individuals (as parts of groups): for example, the right to culture, the right to housing, the right of collective action to an organisation which as another individual entity is representing a collection of individuals. Concepts that are needed to distribute the law may also be available among the following experiences: *res communis* spaces of the planet (Milun, 2011) and UNESCO World Heritage Convention; mechanisms of traditional knowledge and folklore (Chen, 2011); social centre law as a collective law through re-occupation and re-enactement, the right of residence for squatters as a collective through

[22] With the *Pachamama*, the Bolivian government has also been recognising rights to Mother Earth (*Ley de Derechos de la Madre Tierra*), conceptualised as a person, but representing the interests of the collective.

occupation of vacant, abandoned spaces rather than through ownership[23] (Finchett-Maddock, 2011).

It is likely that a distributed law based on common ownership (not on collective ownership by a corporation or a cooperative representing a sum of individuals) will be different from self-management of cooperatives, or social centres, or of the commons as a self-governance method for deliberation and decision-making (and the communal management of resources, being commons-based peer-production, the CBPP of Benkler or of common-pool resources, the CPR of Ostrom). Nevertheless, they can be useful sources of inspiration and provide metaphors to conceptualise collective persons, rights and duties.

Acknowledgments

This research is partially supported by the French ANR (Agency for National Research) through the participation to the ADAM interdisciplinary project on Distributed Architectures and Multiple Multimedia Applications, the Framework programme FP7-ICT-2013-10 of the European Commission through the project P2Pvalue (grant no.: 610961) and the French National Centre for Scientific Research (CNRS) Mission for Interdisciplinarity Programme on Communication Sciences.

I am really grateful to the LSE Department of Media and Communications for hosting me as a Visiting Fellow and offering me the opportunity to discuss this paper during the Research Dialogue. I also thank the members of the LSE Law and Communications Research Network and of the ADAM project for discussions on peer-to-peer and law, and the CNRS Institute for Communication Sciences for supporting my Visiting Fellowship.

[23] Former section 6 of the UK Criminal Law Act 1977.

REFERENCES

Aigrain, P. (2012) *Sharing: Culture and the Economy in the Internet Age*, Amsterdam: Amsterdam University Press.

Antoniadis, P., Le Grand, B., Satsiou, A., Tassiulas, L., Aguiar, R., Barraca, J.P. and Sargento, S. (2008) Community building over Neighborhood Wireless Mesh Networks, *IEEE Technology and Society Magazine* 27(1): 48-56.

Antoniadis, A. and Le Grand, B. (2009) Self-organized virtual communities: Bridging the gap between web-based communities and p2p systems, *International Journal of Web-based Communities* (IJWBC) 5(2): 179-194.

Barlow, J. P. (1996) A Declaration of the Independence of Cyberspace.

Barron, A. (2014) Intellectual Property and the 'Open' (Information) Society, in David, M. and Halbert, D. (ed.), *The SAGE Handbook of Intellectual Property*, London: Sage, forthcoming.

Benkler, Y. (2006) *The Wealth of Networks: How Social Production Transforms Markets and Freedom*, New Haven, CT: Yale University Press.

Boyle, J. (2003) The Second Enclosure Movement and the Construction of the Public Domain. *Law and Contemporary Problems* 66: 33-74.

Brown, I. & Marsden, C. (2013). *Regulating Code: Good Governance and Better Regulation in the Information Age*, Cambridge: MIT Press.

Chen, S.M., Lin, P., Huang, D.-W., Yang, S-R. (2006). A study on distributed/centralized scheduling for wireless mesh network, *Proceedings of the 2006 International Conference on Wireless Communications and Mobile Computing*, 599 - 604. New York: ACM.

Chen, S.-L. (2011) Collaborative Authorship: From Folklore to the Wikiborg. University of Illinois *Journal of Law, Technology and Policy* 1: 131-167.

Dulong de Rosnay, M. (2013). Peer-production online communities infrastructures, *Proceedings of the First Conference on Internet Science*, Brussels: ACM, 65-68.

Dusollier, S. (2011). Scoping Study on Copyright and Related Rights and the Public Domain, CDIP/7/INF/2, Committee on Development and Intellectual Property of the World Intellectual Property Organisation.

Easterbrook, Frank H. (1996) Cyberspace and the Law of the Horse, *University of Chicago Legal Forum*, 207.

Elkin-Koren, N. (2005). What Contracts Can't Do: The Limits of Private Ordering in Facilitating a Creative Commons. Fordham Law Review, 74 (2), 375–422.

Elkin-Koren, N. (2006). "Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic." *New York University Journal of Legislation & Public Policy*, 9 (15), 15-76.

Finchett-Maddock, L. (2011). Observations of the Social Centre Scene: How a Law is Performed through Archiving the Memory of the Commons. PhD Thesis. School of Law, Birkbeck College.

Gilbert, M. (2006). *A theory of political obligation*. Oxford: Oxford University Press.

Gilbert, M. (2nd ed. 1992), *On social facts. London*, New York: Routledge.

Guadamuz, A. (2011). *Networks, complexity and internet regulation scale-free law*. Cheltenham: Edward Elgar.

Giovanella, F. (2014). Liability issues in Wireless Community Networks. Paper presenter at the Final Symposium of the ADAM project, Paris, MINES ParisTech.

Gudynas, E. (2011). Buen Vivir: Today's tomorrow. *Development*, 54(4), 441–447.

Hatcher, J. (2007). Mesh Networking: A look at the legal future. *Journal of Internet Law*, 11(1), 1-16. Preprint available at SSRN: http://ssrn.com/abstract=814984

Jun, J. Sichitiu, M.L. (2003). The nominal capacity of wireless mesh networks, *IEEE Wireless Communications* 10(5): 8-14.

Jondet, N. (2010). The French Copyright Authority (Hadopi): The Graduated Response and the Disconnection of Illegal File-Sharers. Available at SSRN: http://ssrn.com/abstract=1664509

Langheinrich, M. (2001). Privacy by design—principles of privacy-aware ubiquitous systems. *Ubicomp 2001: Ubiquitous Computing*, Berlin Heidelberg: Springer, 273-291.

La Rue, F. (2011). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Office of the United Nations High commissioner for Human Rights, 22 p. http://www.article19.org/data/files/pdfs/reports/report-of-the-special-rapporteur-on-the-promotion-and-protection-of-the-righ.pdf

Latour, B. (2004). *Politics of Nature: How to Bring the Sciences into Democracy*, Cambridge, MA: Harvard University Press.

Lessig, L. (2006). *Code and Other Laws of Cyberspace*, NY: Basic Books.

Lessig, L. (1999). The Law of the Horse: What Cyberlaw Might Teach. *Harvard Law Review* 113: 501-546.

Lindahl, H.K. (2013). We and cyberlaw: The spatial unity of constitutional orders. *Indiana Journal of Global Legal Studies* 20(2): 697-730.

Lovejoy, N. (2011). Procedural concerns with the HADOPI graduated response model. *Harvard Journal of Law & Technology*, 13.

Mansell, R. (2012). *Imagining the Internet: Communication, Innovation, and Governance*, Oxford : Oxford University Press.

Mattei, U. (2013). Economics, Nature and the Commons. *A report on an international conference on the future of the commons*. Organized by the Heinrich Böll Foundation, Commons Strategies Group, Charles Léopold Mayer Foundation and Remix the Commons, Berlin, Germany, May 22-24, 2013. http://www.boell.de/sites/default/files/ecc_report_final.pdf

Milun, K. (2011) *The Political Uncommons. The Cross-Cultural Logic of the Global Commons*, Farnham: Ashgate.

Mowbray, M. (2009) The Fog over the Grimpen Mire: Cloud Computing and the Law. SCRIPTed *Journal of Law, Technology and Society* 6(1): 132-46.

Musiani, F. (2013). *Nains sans géants. Architecture décentralisée et services Internet, Dwarfs without giants. Decentralized architectures and Internet-based services*. Paris: Presses des Mines.

Musiani, F. (2014) Decentralised internet governance: the case of a 'peer-to-peer cloud'. *Internet Policy Review* 3(1). Online: DOI: 10.14763/2014.1.234.

Orsi, F. (2013) Elinor Ostrom et les faisceaux de droits : l'ouverture d'un nouvel espace pour penser la propriété commune, Revue de la régulation, 14(2). Online: http://regulation.revues.org/10471

Ostrom, E. (1990) *Governing the Commons. The Evolution of Institutions for Collective Action*, Cambridge: Cambridge University Press.

Rodotà, S. (2013). Constituting the Commons in the Context of State, Law and Politics, Economics and the Common(s): From Seed Form to Core Paradigm. *A report on an international conference on the future of the commons*. Organized by the Heinrich Böll Foundation, Commons Strategies Group, Charles Léopold Mayer Foundation and Remix the Commons, Berlin, Germany, May 22-24, 2013.
http://www.boell.de/sites/default/files/ecc_report_final.pdf

Sartor, Giovanni (2009). Cognitive automata and the law: electronic contracting and the intentionality of software agents, *Artificial intelligence and law* 17 (4):253-290.

Schollmeier, R. (2001) A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications. *Proceedings of the First International Conference on Peer-to-Peer Computing*, IEEE: 27–29.

Smiley, M. (2011) Collective Responsibility, in Zalta E. N. (ed.) The Stanford Encyclopedia of Philosophy. http://plato.stanford.edu/archives/fall2011/entries/collective-responsibility/

Söderberg, J. (2013) How open hardware drives digital fabrication tools such as the 3D printer. *Internet Policy Review*, 2(2).

Solum, L.B. (1992) Legal Personhood for Artificial Intelligences, *North Carolina Law Review* 70: 1231-1287.

Steinbeis, M. (2012) Occupy the Law!, *Report of the Conference on Transnational Societal Constitutionalism*, Frankfurter Allgemeine Zeitung and VerfBlog. http://ww.verfassungsblog.de/occupy-law

Teubner, G. (2006) Rights of Non-Humans? Electronic Agents and Animals as New Actors in Politics and Law. *Journal of Law and Society* 33(4): 497-521.

Teubner, G. (2007) In the Blind Spot: The Hybridization of Contracting. *Theoretical inquiries in law* 8(1): 51-71.

Teubner, G. & Collins, H. (2011) *Networks as Connected Contracts*, Oxford: Hart Publishing.

von Lohmann, F. (2004) Tracking Pirate in Cyberspace, Symposia—2003 Stanford Law & Technology Association Conference: Ideas without Boundaries: Creating and Protecting Intellectual Property in the International Arena, *Loyola of Los Angeles Entertainment Law Review* 24(1): 73-98.

Media@LSE Working Papers

Media@LSE Electronic Working Papers will:

- Present high quality research and writing (including research in-progress) to a wide audience of academics, policy-makers and commercial/media organisations.
- Set the agenda in the broad field of media and communication studies.
- Stimulate and inform debate and policy. All papers will be published electronically as PDF files, subject to review and approval by the Editors and will be given an ISSN.

An advantage of the series is a quick turnaround between submission and publication. Authors retain copyright, and publication here does not preclude the subsequent development of the paper for publication elsewhere.

The Editor of the series is Bart Cammaerts. The Deputy Editors are Nick Anstead and Ruth Garland. The editorial board is made up of other LSE academics and friends of Media@LSE with a wide range of interests in information and communication technologies, the media and communications from a variety of disciplinary perspectives (including economics, geography, law, politics, sociology, politics and information systems, cultural, gender and development studies).

Notes for contributors:

Contributors are encouraged to submit papers that address the social, political, economic and cultural context of the media and communication, including their forms, institutions, audiences and experiences, and their global, national, regional and local development. Papers addressing any of the themes mentioned below are welcome, but other themes related to media and communication are also acceptable:

- Communication and Difference
- Globalisation and Comparative Studies
- Innovation, Governance and Policy
- Democracy, Politics and Journalism Ethics
- Mediation and Resistance
- Media and Identity
- Media and New Media Literacies
- The Cultural Economy

Contributions are welcomed from academics and PhD students. In the Michaelmas Term each year we will invited selected Master's students from the preceding year to submit their dissertations which will be hosted in a separate part of this site as 'dissertations' rather than as Working Papers. Contributors should bear in mind when they are preparing their paper that it will be read online.

Papers should conform to the following format:

- 6,000-10,000 words (excluding bibliography, including footnotes)
- 150-200 word abstract
- Headings and sub-headings are encouraged
- The Harvard system of referencing should be used
- Papers should be prepared as a Word file
- Graphs, pictures and tables should be included as appropriate in the same file as the paper
- The paper should be sent by email to Bart Cammaerts (b.cammaerts@lse.ac.uk), the editor of the Media@LSE Electronic Working Paper-Series

ISSN: 1474-1938/1946