D6.1 DOMINANT LEGAL CHALLENGES AND SOLUTIONS PRACTISED

Project Acronym:	DiDIY
Project Name	Digital Do It Yourself
Grant Agreement no.	644344
Start date of the project	01/01/2015
End date of the project	30/06/2017
Work Package producing the document	WP6 - Exploring the impact of DiDIY on laws, rights and responsibilities
WP Lead Partner	FKI
Other Partner(s) involved	all
Deliverable identifier	D6.1
Deliverable lead beneficiary	FKI
Due date	M20 (August 2016)
Date of delivery	30/08/2016
Version	1.0
Author(s)	FKI, LIUC
License	Creative Commons Attribution ShareAlike 4.0
Classification	PUBLIC
Document Status	DRAFT
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 644344.	
Disclaimer: The views expressed in this document do not necessarily reflect the views of the EC.	

Disclaimer

This document is provided "As Is"; it is not legal advise, but a study introducing the main research topics in the presented context. We encourage you to further study other sources. Any feedback, suggestions and contributions to make this document better and more useful are very welcome. Please let us know through the contact page http://www.didiy.eu/contact. We will seek to incorporate relevant contributions in the document and add your name to the list of contributors.

Executive summary

Deliverable D6.1, Dominant legal challenges and solutions practised, presents the identified dominant legal challenges to the social diffusion of the phenomenon we call "Digital Do It Yourself" and a series of solutions practised. During the first year of the Project activities, the partners have mapped the key challenges and through a co-design workshop have identified those that they agreed on as the most important ones. Literature review, expert interviews, and case studies have shed light on some of the solutions that are being practised in the field. These have been validated through the Legal Advisory Board (DiDIY LAB). It has become clear through these interactions that many practitioners in the field are in need of guidance on these issues. The information in this deliverable and on the Project's website is aimed at being helpful for various target groups. At the same time, it has become clear that a continued effort after – and not only in parallel to – the lifetime of the Project is highly needed.

After its formal release, updated versions will be made when possible and relevant.

Revision history			
Version	**Date**	**Created / modified by**	**Comments**
0.0	12/07/16	FKI	Draft outline.
0.1	16/08/16	FKI, LIUC	First incomplete draft.
0.2	20/08/16	LIUC	Extensions, fixes, etc.
0.3	22/08/16	FKI	Extensions, fixes, etc
0.4	25/08/16	ABACUS, LIUC	Extensions, fixes, etc
0.5	26/08/16	FKI	Fixes to produce presentable deliverable.
0.6	28/08/16	LIUC	Further revisions.
0.7	30/08/16	LIUC	Further revisions by all partners.
1.0	31/08/16	LIUC	Approved version, submitted to the EC Participant Portal.

Table of Contents

Executive summary....3

Acknowledgements....6

1. Introduction....7
1.1 Purpose, structure, and state....7
1.2 Terms and acronyms....7

2. The nature of DiDIY....9
2.1 Perspectives on DiDIY from the Project's Knowledge Framework....9
2.1.1 DiDIY and individual motivations....9
2.1.2 DiDIY and collaboration....10
2.1.3 DiDIY and open communities and releases....10
2.1.4 DiDIY and free or open access policies....10
2.1.5 DiDIY and Intellectual Property Rights....11
2.1.6 DiDIY and the relation with Free Knowledge & Open Source Hardware....11
2.1.7 DiDIY and the relations between producers and consumers....12
2.1.8 DiDIY and Open Business Models....12
2.2 Ethical values related to DiDIY....13
2.3 A paradigm shift....14

3. Introduction to the core legal systems....16
3.1 Copyrights....16
3.2 Patent rights....16
3.3 Design rights....17
3.4 Trade marks....17
3.5 Contract law....18
3.6 Tort law....18
3.7 Personal Data Protection laws....19
3.8 Telecom regulations....19
3.8.1 Lawful Interception....19
3.8.2 Encryption....20

4. Main Research Topics....21
4.1 Liability....21
4.1.1 Duty of Care....21
4.1.2 The strict liability doctrine....22
4.2 Ownership of DiDIY resources....24
4.2.1 Public domain vs intellectual property....25
4.3 Non-exclusive Public Licensing....25
4.4 3D printing of exclusively protected products and exemptions....27
4.5 Internet of Things and privacy and anonymity....31
4.5.1 Control of personal data....31
4.5.2 Regulation issues....32
4.5.3 Anonymisation....34
4.6 DiDIY Drones....34
4.6.1 What are drones?....34
4.6.2 Comparative perspective: the US overview....35
4.6.3 Working on an EU legal framework....36
4.6.4 National regulations....36

4.6.5 Some provisional conclusions....37
4.7 Blockchain technologies for distributed applications....38
4.7.1 Smart Contracts....38
4.7.2 Decentralised Autonomous Organisations (DAO)....39
4.8 Pathogens and 3D printed guns....40
5. Sharing Knowledge: solutions practised....41
5.1 Licensing Guide....41
5.1.1 Copyleft vs. permissive....41
5.1.2 Free Licenses vs. open licenses....41
5.1.3 FSF-approved “free software” licenses....42
5.1.4 OSI-approved “open source” licenses....42
5.1.5 Free Software licenses....42
5.1.6 Documentation and cultural works licences....43
5.1.7 Hardware designs....44
5.1.8 Hardware certifications....45
5.2 Online Sharing Platforms....46
5.2.1 Software....46
5.2.2 Platforms for sharing hardware designs....46
5.3 Practises to deal with liability....49
6. Further work and conclusions....50
Bibliography....52

Acknowledgements

In addition to the EC support, we are greatly indebted to the following persons and collectives:

- Primavera de Filippi, Malcolm Bain, and other DiDIY Legal Advisory Board members for providing guidance and recommendations;
- Wikipedia for being such a useful collective resource to easily access the most relevant works, concepts and projects in many domains;
- GNU/Linux, LibreOffice, and so many Internet-connected tools for making everybody able to work with a distributed team from many countries in a seamless fashion at the times and places that are most feasible and productive for all the people involved.

1. Introduction

1.1 Purpose, structure, and state

The purpose of this document is twofold: (i) to identify the main legal challenges in the context of Digital DIY (DiDIY), and (ii) to list solutions practised in a set of selected cases. This document is addressed at a wide range of readers, including *policymakers, makers, educators, and entrepreneurs*.

We first describe the nature of DiDIY and its ethical values, and discuss how these relate to the legal domain. The non-exclusive sharing of knowledge in DiDIY communities is allowing participants to lower the costs of R&D and stand on the shoulders of giants, by reusing existing knowledge in the form of software, hardware designs, and documentation. A particular form of that is the sharing of such forms of knowledge as Free Software, Open Source Hardware, and free documentation ("free" refers to freedom, as in free speech, and does not refer to price). Typically in DiDIY practices the sharing of knowledge and making of physical objects occurs outside of the market, i.e., without commercial transactions: people make things by and for themselves, alone but mostly collaborating together.

In this sense we come to observe how such an important legal framework as Intellectual Property Rights[1] (IPR) is challenged by people sharing their knowledge in non-exclusive manners. While the potential for IPR infringement is there, the true challenge is to the foundations of the IPR system itself, when these practices show that creativity can thrive even without the need for exclusive protection of ideas, industrial designs and creative works.

Before addressing the research topics of the main challenges and solutions practised, we introduce briefly the various legal systems that play a key role in these challenges and solutions, ranging from copyright and patents to the protection of privacy and consumers.

We identify then the main challenges and cluster them, ranging from ownership over digital works, to licensing, potential infringements and exemptions, liability, privacy and anonymity, drone regulations, and issues arisen by blockchain technology.

Given the importance of knowledge sharing in the practice of DiDIY, we discuss solutions practised to overcome the hurdles posed by the mainstream legal discipline. Therefore we dedicate one chapter to knowledge sharing, to discuss the range of free and open licensing options currently practised, how designers, makers, and end users deal with the obstacles to sharing.

Some thoughts about further work and conclusions complete this deliverable.

1.2 Terms and acronyms

DIY	Do It Yourself
DiDIY	Digital Do It Yourself
ABC	Atoms-Bits Convergence
IoT	Internet of Things
RT	Research Topic
IPR	Intellectual Property Rights

1 Intellectual Property Rights (IPR) refer to a set of different legal regimes including copyrights, patents, design rights, and trademarks, which are very different to one another. Authors observe that the concept is not unproblematic, as these systems provide certain exclusive rights over intellectual works, which is different from property rights over physical objects.

Free	Adjective from the noun “freedom”, as used in “free speech”; in the context of digital works it refers to works that anyone is allowed to use for any purpose, to modify, share and distribute modified versions of that work; for clarity's sake sometimes “free as in freedom” is used
Gratis	Adjective that refers to something that is “free of charge”, without a price (but can have a cost)
Libre	Adjective from Spanish meaning “free as in freedom” used to refer to “free” in an unambiguous way; the use of this term highlights the fact that only the English language has the ambiguity of free as in freedom and free of charge
Open	Adjective that refers to unimpeded access (cf, “open door”)
Open Source	Adjective that refers to unimpeded access to the source files of a work, enabling anyone to use them for any purpose, to modify, share and distribute modified versions of that work; access to the source code is a precondition for this
FLOSS	Acronym for “Free/Libre Open Source Software” first used for a research project by that name; later used to refer to the full ecosystem of free, libre and open source software projects (likewise the FLOK Society project in Ecuador refers to Free/Libre Open Knowledge Society)

2. The nature of DiDIY

Digital Do-It-Yourself (DiDIY) is a recent socio-technological phenomenon which stems from the widespread availability of digital devices that support the convergence of physical ("atoms") and informational ("bits") components (Atoms-Bits Convergence, ABC), as well as the growing accessibility of related knowledge and data through open online communities. This can lead to the emergence of new scenarios in the roles and relations among individuals, organisations, and society, in which the distinction between users and producers of physical artefacts is blurred, and new opportunities and threats emerge accordingly. The following are excerpts from the DiDIY Knowledge Framework (as developed in the deliverables D2.3, D2.4, and D2.5: the current version is available from the Project website at the page http://www.didiy.eu/project/results) that help us to situate the nature of DiDIY and relate this to the identified legal challenges.

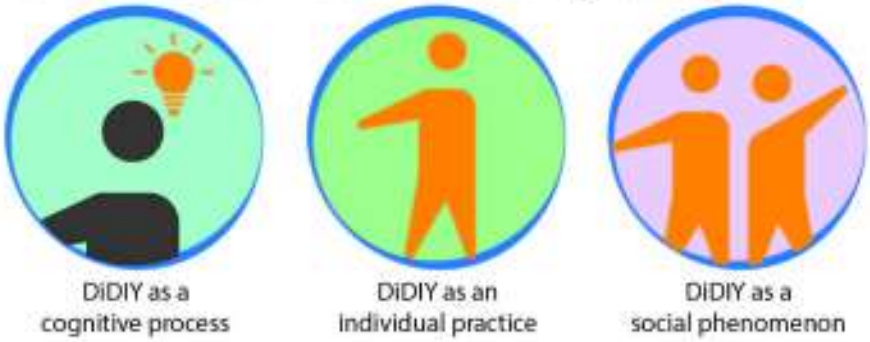

Figure 1 – Three dimensions of DiDIY.

In parallel to the three dimensions pictured in Figure 1, the 'yourself' in DiDIY is originally an individual, but the widespread availability of networked digital information processors and the interest to share knowledge have created new options of DiDIY, in which the yourself can be a group, a class, a community of practice, a company, an industrial cluster, the society as such. The collaboration is set up not only in face-to-face situations but also through:

- *transmission networks* (from the Internet to the Internet of Things), that enable
- *communication and design networks* (sharing digitally coded information on texts, music, images and videos, geo-localisation of objects, shapes of objects, ...), that enable
- *collaboration networks* (thus intended as social, technologically-enabled systems).

Such networks are thus the effective enablers that make DiDIY not only a cognitive process or an individual practice but also an important social phenomenon.

In the following paragraphs we will mention some of the key characteristics of DiDIY.

2.1 Perspectives on DiDIY from the Project's Knowledge Framework

2.1.1 DiDIY and individual motivations

In a narrower view DiDIY refers to established members of the "maker" community who operate according to an ethical principle, while in a broader view it includes all people who at some point or another choose to engage in the practice of DiDIY to some degree, independently of their individual motivations.

The possible motivations that move an individual toward DiDIY are many and different, and may be related to ethical principles (e.g., concern for the environment), but also to a desire to save money, develop new skills, acquire social reputation, etc.

2.1.2 DiDIY and collaboration

In a narrower view DiDIY is about activities carried out by one person (the "yourself"), while in a broader view it is also about collaboration (the plural form of "you", also known as "Do It With Others", DIWO, or "Do It Together", DIT) and transdisciplinarity.

By taking a broader view, one can find almost always some form of collaboration, as even the individual maker builds on previous knowledge produced by others. The individual can be seen as standing on the shoulders of giants: building on collective works produced and shared within (online) communities, typically by many others.

2.1.3 DiDIY and open communities and releases

In a narrower view DiDIY is about openly sharing knowledge in communities and openly released outcomes, while in a broader view it is also of individuals operating alone and about outcomes that are maintained proprietary.

The legal rights under which the digital files are shared determine the affordances that users in these communities have, and thus their possibilities to use, reuse, share, adapt and become economically sustainable. Liberal licensing schemes like free and open licensing are typical in online design sharing platforms, as they convey the maximum freedom or rights to their peers (for an overview of online design sharing platforms in the context of DiDIY, see http://wiki.freeknowledge.eu/index.php/Design_Sharing_Platforms).

2.1.4 DiDIY and free or open access policies

In a narrower view DiDIY is associated with opening the source of personal projects with a generic use and redistribution license and enabling collaboration through communities offering distributed revision control, while in a broader view it is associated with the informal sharing of a project, or just its outcomes, to an online community or social network, leaving the access policy just undefined.

The effectiveness of DiDIY through transmission → communication → collaboration networks has been emphasised and accelerated by the availability of free or open access policies:

– at the transmission level, the protocols of the TCP/IP stack, that constitute the technical foundation of the Internet, are freely licensed and open by design;

– at the communication and design level, both digital, machine-ready designs and the documentation needed to learn how to produce, modify, and use them can be freely shared, sometimes in open formats, that can be processed with free of charge, low-cost software of third parties, accessible to everybody with a computer, not just with expensive applications by the inventor and sole "controller" of the file format;

– at the collaboration level, projects can be developed, shared and reused quickly, without paying royalties and/or going through complicated, expensive legal/bureaucratic procedures, or generally asking for permission, and at global scale in the logic of open collaboration and innovation (open source communities, IPR management via Creative Commons licensing, etc).

2.1.5 DiDIY and Intellectual Property Rights

In a narrower view DiDIY is about sharing designs, instructions and documentation under non-exclusive conditions, while in a broader view it can also include exclusively controlled forms of knowledge.

DiDIY may be specifically about sharing designs, instructions and documentation under non-exclusive conditions, even though the current Intellectual Property Rights (IPR) legislation tends to restrict this kind of sharing by default (e.g., copyright is granted as all rights reserved by default). In this sense, the IPR system is the first one being challenged by DiDIY practices, and not necessarily by infringing exclusive rights in patents or copyright, but by questioning the foundation of IPR itself. It is based on the hypothesis that creators and inventors need to have exclusive control over their works. The open sharing under free licenses of software, hardware design, documentation and instructions has shown that exclusive control over a developer's work is not a necessary condition for such works to be created (and in abundance). In a broader view, however, DiDIY can also include exclusively controlled forms of knowledge, including the use of patented tools and designs or documentation that can be used for only certain practices of DiDIY.

2.1.6 DiDIY and the relation with Free Knowledge & Open Source Hardware

In a narrower view DiDIY knowledge is shared freely within communities, while in a broader view DiDIY projects may come also with non-free conditions.

One of the foundational principles of DiDIY is the sharing of knowledge. While DIY is something that one person theoretically can do completely alone and keep private, DiDIY practically always involves some form of knowledge sharing (imagine that someone buys a household 3D printer or an electronics product that helps them set up a little sensor network for themselves: even if they are proprietary systems, in some way some shared knowledge is involved).

In the narrower view knowledge is shared freely within DiDIY communities. Most typically this occurs through online knowledge sharing platforms that are open for participation and share knowledge about techniques, solutions and projects providing certain rights to other users. Very typical are projects classified as Free Knowledge, Free Software, Open Source Software, Open Source Hardware, or Free Cultural Works. These are different terms for expressions of knowledge ("works") that are shared with the following four freedoms:

a) the freedom to use for any purpose;

b) the freedom to study and adapt to one's needs;

c) the freedom to copy and share with one's neighbour, and

d) the freedom to distribute modified versions.

In a broader view, DiDIY knowledge sharing at least requires access to the ideas and the possibility to adapt these to one's needs. DiDIY projects may come with non-free conditions. One restriction that may apply is the non-commercial one (e.g., under the CC BY-NC license), which limits the use or sharing of the works to non-commercial contexts. DIY typically is done for solving a person's or group's problems and not directly commercial exchange (though selling of the results may occur). Another restriction that sometimes is used is a non-derivative restriction (e.g., CC BY-ND), which restricts users from distributing modified versions. When one or more of such restrictions apply, these works cannot be considered "free" (as in freedom) nor "open" (as in "open source") and thus they would not be part of the collection of free knowledge. The use of free licenses – that guarantees the mentioned four freedoms – is often a considerable advantage for communities to become

sustainable and common under practitioners of DiDIY. This relates also to the sustainability and business models.

2.1.7 DiDIY and the relations between producers and consumers

In a narrower view DiDIY only involves cases in which the producer of an item is also its consumer, while in a broader view it can also include cases in which these two roles remain separate (such as with a hobbyist occasionally selling 3D printed items to others).

As both an activity and a mindset, DiDIY further blurs the distinction between producers and consumers that is already a characteristic of DIY, leading to the concept of a "prosumer" (Toffler 1980): a person who combines the roles of producer and consumer with regard to one and the same product.

2.1.8 DiDIY and Open Business Models

In a narrower view DiDIY knowledge production occurs voluntary between peers with no commercial transaction nor immediate business model, while in a broader view DiDIY projects may come also with a range of revenue models.

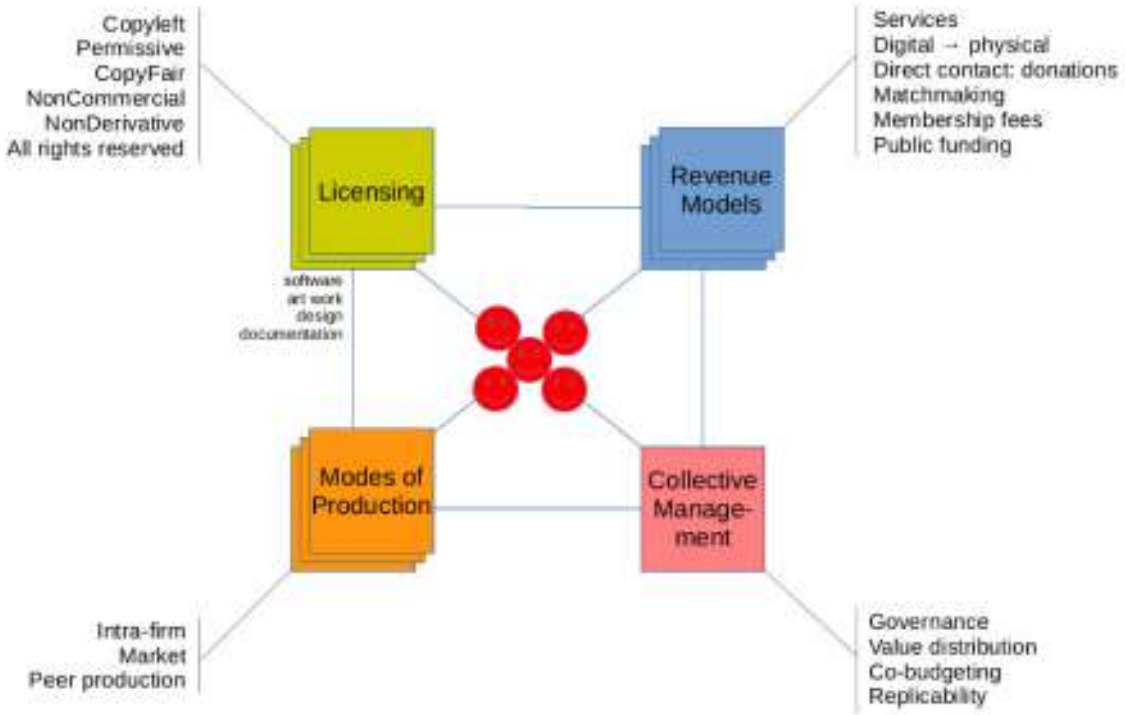

Figure 2 – Open Business Models.

While the knowledge sharing may occur under free licenses and without monetary exchange, there is still a range of options to generate revenues. Revenue models include typically:

– *added value services*, e.g., to provide training, workshops, consultancy;

– *direct contact*, where income is generated through direct contact between producers and consumers, through donations or crowdfunding;

– *matchmaking platforms*, where supply and demand are brought together and the platform typically charges a small percentage over the transactions;

– *membership fees or cost sharing*, where associations of people share the cost of the collective;
– *public funding*, where public institutions provide subsidies or otherwise contribute economically.

2.2 Ethical values related to DiDIY

In the Knowledge Framework we have identified some of the core ethical values practised, as is shown in the following excerpt.

In a narrower view DiDIY concerns the ethical issues raised by the practice of DiDIY itself and the guidelines to be followed to engage in it in an ethically desirable manner, while in a broader view it also involves studying the values and convictions that tend to prevail among DiDIYers and to govern their activities.

The core values behind the characteristics of DiDIY, as described in the Knowledge Framework, emphasise the importance of (i) the value of sharing and helping others (solidarity), (ii) the reputation economy (trust, transparency, demonstration of skills), (iii) equal rights of access and participation (equity), and (iv) the fact that participants do not need to obtain permission (free-as-in-freedom, autonomy). These values may not be necessarily shared by all, but they can be seen as present in most, if not all, of the DiDIY communities.

Referring to (i), online creation communities are characterised as places where people share knowledge and help each other, through platforms like online forums and file repositories. Even when digital resources created in such fashion are shared freely, i.e., not for money, they can be valuable, although this value is not measured according to traditional theories of (market) value: the reputation economy, i.e., the value of peers gaining reputation, is considered important (ii). Indeed, studies of Free Software communities consider reputation as one of the important motivational factors for developers to share their code (Bonaccorsi 2003).

Observing the increased use of free and open licenses over the last years – the sum of Creative Commons licensed works alone has reached the number of 1 billion works in 2015[2] –, we can relate this to a growing importance for equal rights (iii), as granted by free licenses. More specifically looking at platforms where people share works in the context of DiDIY, we find a domination of free and open licenses. This indeed can be expected from the DIY culture, where autonomy and freedom are considered a cornerstone (iv). At the same time, many of such platforms, while encouraging sharing under free or open licenses, themselves are not replicable and their governance often is not participatory, or is limited to receiving feedback from the community. The EC funded P2Pvalue project[3] has shown that more self-governance favours mission accomplishment and community building and value creation in areas linked to physical sharing of spaces, such as FabLabs.

Additionally, communities of DiDIY can be observed to have an increased awareness for responsibilities to care for others, inherent to community values. This feature could help to address the legal concept of "duty of care" further discussed in this deliverable, to transmit warnings and knowledge of risks between all participants in the chain of ideation → design → development → production → usage.

2 See the State of Creative Commons 2015: https://stateof.creativecommons.org/2015.
3 The P2PValue project, funded under the EC CAPS programme, studied more than 300 online communities of varying degrees of commons-based peer production: https://p2pvalue.eu. The directory of cases studied: http://directory.p2pvalue.eu.

2.3 A paradigm shift

Although several scholars, futurists, and visionaries talk about the emerging paradigm, "Third Industrial Revolution", "Industry 4.0", "Post-capitalism", and a long etcetera, none of us can predict the future. However, we can identify several trends and key concepts that are changing the socio-economic foundations of our societies. It is relevant to see the changing rights and obligations in the light of these trends. Ultimately it is this kind of changes that provokes the challenges and tensions that we are studying:

- *network society*: all Internet-connected human beings can connect to each other directly, thus leading to disintermediation effects;
- *end-to-end communication*: the Internet is based on the principle that users can deploy any desired protocol between different endpoints, thus allowing innovation to occur at the edges of the network;
- *open standard protocols*: while proprietary protocols, as, e.g., Skype, do exist, the dominant use is over open standard protocols, that anyone can use and implement freely;
- *network effect*: the so-called "Metcalfe's Law" describes the effect that one user of a good or service has on the value of that product to other people. An example is the telephone network: when only two phones are connected, one connection can be established; the more phones, the more connections can be made and thus the more value the network has to every phone owner, and in consequence to the network owner;

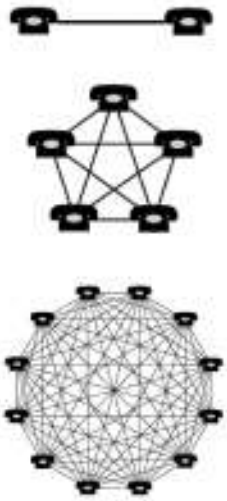

Figure 3 – The network effect in a few simple phone networks (author: Fernando S. Aldado).

- *distributed digital networks* with near zero marginal cost replication: as in the case of file sharing, copying a file in a distributed network only adds the energy cost, when all physical resources are in place. The BitTorrent protocol is an example of a distributed file sharing network: when more people connect to download a given file, they themselves become nodes in the network and share part of the workload, thereby strengthening the network by increasing speed and value;
- *near zero marginal costs*: it refers to the general concept of a production cost that is almost zero for adding additional units of a product or service. Examples are digital commons resources, such as GNU/Linux or Wikipedia that can be copied for an insignificant cost compared to their development, and renewable energy installations that, once installed, have

a very low operating cost. An increasing part of the economy is absorbed by "zero marginal costs webs" produced by online "collaborative commons" such as Jeremy Rifkin calls them (Rifkin 2015);

- *from mass production towards mass customisation*: small scale production is becoming increasingly economically viable;
- *digital commons*: they are collectively constructed and maintained resources that can be replicated and reused freely, typically under free licenses. Commons are considered a third form of property and a third model of governance alongside private and public property, and commons-based peer production a third mode of production (Benkler 2002), (Bauwens 2005). With the rise of the Internet we can see also a rise of this third model, strongly digitally mediated, in examples like Wikipedia, the Free Software Movement, and the collaborative or sharing economy;
- *ecosystem awareness*: human beings have become aware of the human caused nature of climate change and therefore the urgency of radical changes. In product design we can appreciate cradle-to-cradle or circular economy, to close the loop of product lifecycles through greater efficiency and reuse. In 2015 the European Commission has started a full Circular Economy Action Plan[4]. The rise of distributed production of energy, informational and physical goods fits with this trend.

4 EC Circular Economy Action Plan (2-12-2015): http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52015DC0614.

3. Introduction to the core legal systems

In this section we will describe the core legal systems that are relevant for different aspects of the DiDIY phenomenon. The intention is to provide an accessible introduction for non-lawyers.

3.1 Copyrights

Copyright is a legal right created by the law of a country that grants the creator of original work exclusive rights for its use and distribution, usually only for a limited time. Such rights are not absolute but have limitations and exceptions, including fair use. A major limitation on copyright is that copyright protects only the original expression of ideas, and not the underlying ideas themselves[5].

In most legislations, copyright is obtained automatically (i.e., without registration) when a work is made public and meets minimal standards of originality in order to qualify for copyright.

By default, the author of a work becomes the owner of the copyrights over that work, which gives him or her exclusive rights over, e.g., the production of copies, the distribution or sale, the modification and making of derivative works, the selling of these rights to others. All these exclusive rights can be considered when authors publish their work when stating "All rights reserved", and even without that statement they may apply[6].

3.2 Patent rights

A patent is a document, issued, upon application, by a government office (or a regional office acting for several countries), which describes an invention and creates a legal situation in which the patented invention can normally only be exploited (manufactured, used, sold, imported) with the authorization of the owner of the patent. "Invention" means here a solution to a specific problem in the field of technology. An invention may relate to a product or a process. The protection conferred by the patent is limited in time, generally 20 years[7].

Simply put, a patent is the right granted to an inventor to exclude others from commercially exploiting the invention for a limited period, in return for the disclosure of the invention, so that others may gain the benefit of the invention. The disclosure of the invention is thus an important consideration in any patent granting procedure.

Patents may be granted for inventions in any field of technology, from an everyday kitchen utensil to a nanotechnology chip. An invention can be a product, such as a chemical compound, or a process, such as a process for producing a specific chemical compound. Many products in fact contain a number of inventions. For example, a laptop computer can involve hundreds of inventions, working together[8].

5 Daniel A. Tysver, Works Unprotected by Copyright Law: http://www.bitlaw.com/copyright/unprotected.html#ideas.
6 For more sources see https://en.wikipedia.org/wiki/Copyright.
7 WIPO Intellectual Property Handbook: Policy, Law and Use. Chapter 2: Fields of Intellectual Property Protection: http://www.wipo.int/export/sites/www/about-ip/en/iprm/pdf/ch2.pdf.
8 World Intellectual Property Organization, Patents: Frequently Asked Questions: http://www.wipo.int/patents/en/faq_patents.html.

3.3 Design rights

Design right protects the shape of a three-dimensional design. It subsists if the design is recorded on paper, or if a product has been made according to that design. It has rules on qualification for protection by both citizenship of the designer and place of the designing[9].

'Design' here means the appearance of the whole or a part of a product resulting from the features of, in particular, the lines, contours, colours, shape, texture and/or materials of the product itself and/or its ornamentation. 'Product' means any industrial or handicraft item, including inter alia parts intended to be assembled into a complex product, packaging, get-up, graphic symbols and typographic typefaces, but excluding computer programs. 'Complex product' means a product which is composed of multiple components which can be replaced permitting disassembly and re-assembly of the product.

Design right does not subsist in parts of a design necessary to connect to another article, to surface decoration, to methods and principles of construction or to those parts of a design which are dependent on the appearance of another article, where that article and the article that design right applies to is an integral part of the second article. Design right also does not apply if a design is not original, and a design is defined as not being original if the object so designed is commonplace in the field when designed.

The European Union has two important directives on design rights: the 1998 Design Directive (DD) and the 2002 Community Design Regulation (CDR)[10]. The DD was enacted with the goal of harmonising the – sometimes significantly heterogeneous – national legislations of Member States in the field of registered design products (Margoni 2013). The CDR provides a registered option of Registered Community Design (RCD) and also an unregistered option, Unregistered Community Design (UCD).

A key aspect of the CDR is the unitary character of protection, which mandates that a community design shall have equal effect throughout the Community and can only be registered, transferred, or surrendered or be declared invalid in the whole European Community. The CDR also mentions certain limitations: "Technological innovation should not be hampered by granting design protection to features dictated solely by a technical function. It is understood that this does not entail that a design must have an aesthetic quality. Likewise, the interoperability of products of different makes should not be hindered by extending protection to the design of mechanical fittings. Consequently, those features of a design which are excluded from protection for those reasons should not be taken into consideration for the purpose of assessing whether other features of the design fulfil the requirements for protection".

3.4 Trade marks

A trade mark is a sign aimed at distinguishing the goods and services of a party from those of its competitors (the party may refer to its trade mark as its "brand")[11]. The writing of the term as one word is common in the USA: a "trademark" is a word, phrase, symbol, and/or design that identifies and distinguishes the source of the goods of one party from those of others[12].

9 UK Copyright, Designs and Patents Act 1988: http://www.legislation.gov.uk/ukpga/1988/48/contents.
10 Council Regulation (EC) no 6/2002 of 12 December 2001 on Community Designs: http://euipo.europa.eu/en/design/pdf/reg2002_6.pdf.
11 https://www.gov.uk/guidance/unacceptable-trade-marks.
12 United States Patent and Trademark Office, USPTO: http://www.uspto.gov/trademarks-getting-started/trademark-basics/trademark-patent-or-copyright.

A European Union trade mark, or EU trade mark (abbreviated EUTM; named Community Trade Mark (CTM) until 23 March 2016), is a trade mark which is pending registration or has been registered in the European Union as a whole, rather than on a national level within the EU.

The EU trade mark system creates a unified trade mark registration system in Europe, whereby one registration provides protection in all member states of the EU. The EU trade mark system is unitary in character. Thus, a EU trade mark registration is enforceable in all member states, while an objection against a EU trade mark application in any member state can defeat the entire application.

While the trade mark law seeks to protect indications of the commercial source of products or services, patent law generally seeks to protect new and useful inventions, and design rights generally seek to protect the look or appearance of a manufactured article. Trade marks, patents, and designs collectively form a subset of intellectual property known as *industrial property* because they are often created and used in an industrial or commercial context.

3.5 Contract law

A contract is a voluntary arrangement between two or more parties that is enforceable at law as a binding legal agreement. Contract is a branch of the law of obligations in jurisdictions of the civil law tradition. A contract is "a promise, or set of promises, for breach of which the law gives a remedy, or the performance of which the law in some way recognizes as a duty" (Williston 1959). The essentials of a valid contract are parties competent to contract, a proper subject-matter, consideration, mutuality of agreement, and mutuality of obligation.

A contract arises when the parties agree that there is an agreement. Formation of a contract generally requires an offer, acceptance, consideration, and a mutual intent to be bound. Each party to a contract must have capacity to enter the agreement.

Contracts are used for many forms of economic exchange, one of them being the transfer of copyright or other exclusive rights, e.g., from (individual) authors to publishers exploiting their works. Another relevant example is when authors decide to publish their works under a free license: the users or licensees in many cases can be considered to enter into contract with the authors of the work in order to obtain the rights granted in the free license.

3.6 Tort law

Tort law consents to individual victims of wrongdoing a right of action and a set of remedies against the individuals who wronged them (Sherwin 2011, p.227).

According to Roman law tradition, followed mainly in Continental Europe, the traditional principle of "neminem laedere" states that any intentional or negligent act that causes an unjustified injury to another obliges the person who has committed the act to pay damages. If the damage originates from a crime, the legal system generally provides for compensation of moral damages.

In Common Law tradition, a tort is a civil wrong that unfairly cause losses or harms to someone. The tortfeasor, i.e., the person who commits the tort, results to be liable for the unfair act committed. In this perspective, a civil legal action represents the organised scheme for determining where and under what condition the monetary costs of a harm should be paid by the tortfeasor by an authoritative (mainly a judicial court) order (Malone 1970, p.1).

3.7 Personal Data Protection laws

The right to privacy is a crucial element of our personal security, for free speech and for democratic participation. It is a fundamental right in the primary law of the EU and is recognised in numerous

international legal instruments. Digital technologies have generated a new environment of potential benefits and threats to this fundamental right.

Different regulations affect personal data, privacy and anonymity, including:

- *Personal Data Protection Directive*[13]: under EU law, personal data can only be gathered legally under strict conditions, for a legitimate purpose. Furthermore, persons or organisations which collect and manage your personal information must protect it from misuse and must respect certain rights of the data owners which are guaranteed by EU law;
- *Data Retention Directive*: it compels communications service providers routinely to capture and archive information detailing the telephone calls, web surfing, e-mail messages, and other communications of their users for a period between 6 months and two years.

3.8 Telecom regulations

Apart from the Personal Data Protection and Data Retention Directives, that directly regulate Internet Service Providers on how to deal with their customers data, other regulations apply.

3.8.1 Lawful Interception

One example of Telecom-related regulations that may have a direct impact on certain kinds of DiDIY activities are those that regulate Lawful Interception, and the corresponding constraints on telecom equipment and operators.

Lawful Interception (LI) is *"a legally sanctioned official access to private communications"*[14]. LI laws describe "*the process by which law enforcement agencies conduct electronic surveillance of circuit and packet-mode communications as authorized by judicial or administrative order. Countries throughout the world have adopted legislative and* regulatory requirements *for providers of public and private communication services (service providers) to design and implement their networks to* support authorised electronic surveillance explicitly"[15].

LI implementation is required by the EU International User Requirements 19951 which allows for LI to prevent crime, including fraud and terrorism[16]. In the US, the Communications Assistance for Law Enforcement Act (CALEA) plays a similar role.

DiDIY technologies, practices and communities can be also used to build and operate bottom-up, community telecom networks. Two of many examples in this area are the LoRaWAN technology used by The Things Network community[17] all around the globe and the Guifi.net[18] community Internet operated by more than 30.000 homes, offices and institutions. Regardless of the specific norms, there is a direct impact of LI on such cases and vice-versa. On one hand, imposing LI compliance on these networks and the underlying DiDIY projects may put an unbearable burden on them, seriously limiting their adoption. On the other, as already mentioned with IPR legislation, DiDIY, or bottom-up self-organised telecom networks, often without any central "service provider", question the very foundations and applicability of Lawful Interception.

13 http://www.eeas.europa.eu/data_protection/index_en.htm.
14 LTE World: http://lteworld.org/blog/lawful-interception-architecture-lte-evolved-packet-system.
15 www.cisco.com/c/en/us/tech/security-vpn/lawful-intercept.
16 www.etsi.org/technologies-clusters/technologies/security/lawful-interception.
17 See for example: http://freeknowledge.eu/blogs/now-lora-building-smart-city-bottom-up.
18 Guifi.net was awarded the first European BroadBand Award by the EC for its innovative financing and management model: http://catalannewsagency.com/society-science/item/catalan-internet-project-guifi-net-wins-european-broadband-award.

3.8.2 Encryption

A similar consideration applies to encryption-related regulations or proposals, like the Burr-Feinstein bill in the US[19] or the ""anti-terrorism" legislation" approved in June 2016 in Russia[20]. Even court orders like those requested by the FBI in the "San Bernardino" case[21] may be much more difficult to request and apply, in a DIWO/DIT scenario.

For the moment, the EU has a different approach. In March 2016 the EU cybersecurity agency ENISA "spoke out against creating backdoors for law enforcement agencies to access encrypted communication"[22]. However, in August 2016, the French Interior Ministry argued that "the European Commission (EC) should draft a new law that would require companies to work with the authorities to decrypt secure communications on demand and help track down terrorist suspects"[23].

19 http://www.dailydot.com/layer8/senate-encryption-bill-crypto-wars-backdoors-burr-feinstein-official-release.
20 http://www.dailydot.com/layer8/encryption-backdoor-russia-fsb-bill-passes.
21 https://cdt.org/insight/issue-brief-a-backdoor-to-encryption-for-government-surveillance.
22 *https://www.euractiv.com/section/digital/news/eu-cybersecurity-agency-slams-calls-for-encryption-ackdoors.*
23 *http://www.theregister.co.uk/2016/08/24/french_german_ministers_call_for_new_encryption_backdoor_law.*

4. Main Research Topics

WorkPackage 6 of this Project studies the rights and responsibilities that users and producers of DiDIY-related technologies have and how current legislation affects them and vice versa.

On 14 July 2015 the Project partners participated in a co-design workshop to collectively discover the various topics that make up the challenges in the context of impact of DiDIY on laws, rights and responsibilities**.** The session was co-organised by FKI and POLIMI and included the participation of representatives of all partners[24].

The main challenges identified mark the set of Research Topics (RTs) that WP6 aims to explore. The relevance of these RTs has been validated by the Project's Legal Advisory Board.

An initial exploration of some of these RTs has been published while preparing this deliverable (Falletti, Tebbens 2016).

4.1 Liability

For taking the concept of liability into account in the context of DiDIY at least two underlying concepts have to be discussed: 1) duty of care, and 2) product liability or the so called "strict liability doctrine".

4.1.1 Duty of Care

The legal expression "tort law" refers to "a body of rights, obligations, and remedies that is applied by courts in civil proceedings to provide relief for persons who have suffered harm from the wrongful acts of others"[25]. In this situation there is a specific legal area of interest: the "duty of care" rule. A well-known opinion written by Lord Atkin in the famous case "Donogue vs. Stevenson" [1932] UKHL 100 (26 May 1932) defines what exactly duty of care is: "You must take reasonable care to avoid acts or omissions which you can reasonably foresee would be likely to injure your neighbour. Who, then, in law, is my neighbour? The answer seems to be – persons who are so closely and directly affected by my act that I ought reasonably to have them in contemplation as being so affected when I am directing my mind to the acts or omissions which are called in question.".

The rule of duty of care is fundamental for understanding the negligence doctrine, under which every person involved in a DiDIY making is liable for his or her amateur production. It has to be distinguished from product liability rules, that pertain to professional producers' and consumers' commercial relationships. It is a matter of burden of proof in litigation. In fact, in case of duty of care and negligence, the plaintiff has to demonstrate the negligence of the non-professional maker. In case of product liability the professional producers are liable according to strict liability rules.

The rule of duty of care is a shared legal principle both in civil law and common law tradition. It represents a fundamental principle for ensuring a peaceful "living together" in society. Indeed, the duty of care principle assures the accountability of the people involved in the production of goods and services.

---

24 Workshop participants: for LIUC: Luca Mari, Aurelio Ravarini, Fernando Alberti, Luca Cremona, Elena Falletti, Jessica Giusti, Paola Negrin, Emanuele Pizzurno, Emanuele Strada; UOW: David Gauntlett; ABACUS: Enrico D'Amico, Maria Bulgheroni, Roberto Rossi; MMU: Bruce Edmonds; FKI: Wouter Tebbens, Marco Fioretti; AC: Vincent Muller, Alexander Erler; POLIMI: Marita Canina, Laura Anselmi, Carmen Bruno, Elisabetta Coccioni, Giuseppe Salvia, Valentina Rognoli.

25 http://legal-dictionary.thefreedictionary.com/Tort+Law.

Normally, product liability refers to the liability of a seller or a producer of a product when there is consumer personal injury or his or her property damage is caused by a product defect (Berkowitz 2015). However, the widespread social diffusion of 3D printing, and digital fabrication more generally, is making the traditional boundaries between producers and consumers blur and this is giving rise to liability issues for which legal solutions are not clearly determined yet neither in the EU nor in the US legal systems (DeClercq 2015).

Under this perspective both CAD files and 3D printed items could be categorised as products, provided that they are distributed commercially for use or consumption (Wang 2016). It should be noted however that this is not the case for non-exclusive sharing, or more generally when there is no trade.

4.1.2 The strict liability doctrine

In the current legal framework, product liability refers to three categories of defects: manufacturing, design, and warning defects (Wang 2016).

Let us consider an example: at a request of a friend, a hobbyist maker produces a spare part of an object commonly used in a household: a lounge chandelier arm. It is designed reusing design files that were shared by another designer through an online design sharing platform through CAD software adapting it by by another friend, a design passionate, and produced with the maker's 3D printer. After some time, the spare part proves defective and causes the fall of the chandelier itself hurting one of the children of the maker's friend. Who is liable for this accident? Who made mistakes and might be held liable to pay damages? The point is that the 3D printer itself, the parts and materials chosen by the maker to build it, or the way the printer is assembled, maintained and used, may all be other reasons why the final product proves defective, even if the CAD design was perfect.

Since the DiDIY environment uses tools such as 3D printers to produce physical objects, it is evident that such legal issues also interest the non-professional makers. In the US legal system product liability is referred to the application of the strict liability doctrine. According to it, "one engaged in the business of selling or otherwise distributing products who sells or distributes a defective product is subject to liability for harm to persons or property caused by the defect", without having to carry the burden of proof of the negligence in the production of the defective product. According to the same doctrine a product is "defective" if it has a manufacturing or design defect or if it is accompanied by an inadequate set of instructions or warnings.

According to scholars, "the theory underlying the imposition of strict product liability is threefold: (1) those who manufacture and sell products tend to be enterprises; (2) imposing liability on enterprises is fair because those who profit from the risk should bear the costs of accidents; and (3) enterprises are better than injury victims at absorbing and distributing losses". However, the DiDIY environment could satisfy only part of these conditions: 1) DiDIY makers are not usually professionals or enterprises, as more typically they are amateurs or hobbyists; 2) normally they take no profits from making their products, but 3) their products could be affected by production defects or cause harm and damage. In this perspective scholars opine that home-made products could "fall outside the scope of strict liability" (Freeman Engstrom 2013), (Osborn 2014). Accordingly, "a simple negligence standard may be more equitable depending on the circumstances because the majority of these sellers are small, sole proprietorships" (Nielsen 2015). However, strict liability rules could be applied on specific cases, depending when an entity is a regular seller, rather than an occasional or casual one.

In the EU, the product liability rule is quite similar and refers to strict liability. Indeed, according to Article 3 of the Directive 85/374/EEC[26] on product liability, "producers" are those who manufacture a product and put it into circulation (Erler 2015). However, according to Article 7 letter c) of the same Directive, the producer shall not be liable if he proves "that the product was neither manufactured by him for sale or any form of distribution for economic purpose nor manufactured or distributed by him in the course of his business". While this exception could be applicable to DiDIY makers, there are no specific published case laws on this issue.

In the above mentioned case of the lounge chandelier arm, there can be different potential defendants according to the different roles played by the people involved in the manufacturing process depending by their role (Wang 2016). For the plaintiff it could be very difficult and expensive to verify the burden of proof of each of them. Scholars provided a good number of examples, for instance the case of the occasional inventor or the hobbyist program designer who creates CAD files, uploads them to the Internet to be used by others for non-commercial purposes. At the same time, the maker could use raw materials not appropriate for the intended use (Wang 2016, p.107).

It seems possible wondering if it is more equitable to flip the traditional prospect related to the burden of proof for facing these complications and enhancing the protection of weak parties. Instead of giving to the injured parties (i.e., the plaintiff in a possible litigation) the burden of proof, at least in specific cases that will need further study it could be more appropriate to apply by extending to them the rules on consumer protection. It is a matter of policy choices as to which social part has to be protected: individual initiative of those who tend to explore an innovative technological field or the legal protection of the final product user? It can happen that in some cases the two figures – amateur producer and final consumer – coincide, but the opposite may happen, when the DiDIY amateur producer gives away self-made products even within the circle of his or her family or his or her friends. Also the amateur producer may use DIDIY in his/her professional activity, like the dentist 3D printing her own dental crowns or a daycare manager CNC milling wooden toys for his playground.

According to a scholar, "(A)cting as the consumer and manufacturer, the user must accept the responsibilities of both parties" (Harris 2015, p.6).

Some preliminary considerations can be then proposed: from the consumer's point of view, he or she must use the product, even if made by an amateur, according to the use that has been designed by its creator. The effects of inappropriate use of that product shall be borne only by the consumer, because of his or her choices. In this regard, and from the manufacturer's point of view, he or she must arrange appropriate warnings and instructions on the use of the product itself (Harris 2015, p.6). According to the same scholar point of view "product liability law has two main purposes: to provide injured consumers with compensation through a third-party accident insurance system imposed on manufacturers to spread the risk and to improve product safety by reducing the production of dangerous products" (Harris 2015).

For example, the application of DiDIY in the medical care and bioprinting of human organs could represent a good example of liability application. While both EU and US have a strong legislation in medical care products, experimental and prototyping applications could be seen as an opportunity for DiDIY makers. Who can be held liable in case of damage due to a design defect? A distinction should be made here between professional and non-professional makers: professional makers are treated under strict liability rules, while both the non-professional figure and non-commercial seller of "print-at-home" objects are liable only in case of negligence, under duty of care.

26 http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A31985L0374.

Subscribing an insurance contract to cover the consequences of accidents occurring due to the use of DiDIY products could be a solution for balancing the need of protection of the user of the DiDIY products from the consequences of mistakes and defects of the hobbyist manufacturer.

4.2 Ownership of DiDIY resources

Digital resources produced in the context of DiDIY range from software code to documentation, from blueprints to design files, from protocols to data. For intellectual or creative works there are two forms of ownership. The first one is of the possible exclusive rights granted by any one of the different intellectual property right regimes. In the case of copyright: for that to subsist there must be the appropriate creative effort or originality present in the artistic work. If this is present, the author obtains the exclusive rights as defined in copyright law when making the work public. Patent rights or trademarks should be requested, and, if granted, the patentee or trademark holder will be the owner over those rights. The second form of ownership is the physical form of the work, say of one "instance" or copy of the work, be it one book, one product, one copy of the software. While the rights holder is the owner of the exclusive rights, once he or she distributes, i.e., sells, a copy, the exclusive rights are exhausted. This is what in US law is called the "First Sale Doctrine", and allows the buyer to resell the copy of the book, software or patent protected product without suffering infringements. The doctrine is also referred to as the "right of first sale", "first sale rule", or "exhaustion rule".

In the case of digital resources that are produced by a community of peers, there can be many contributors. The ownership of collectively constructed digital resources is however not simply between public and private goods. Following the model of commons-based peer production[27], it is a community of peers that co-produce a common resource that can be used by all under equal conditions.

In these cases of peer produced resources, it can be difficult to answer who is the owner of such resource. On the one hand, each contributor may have authorship and therefore generally part in the ownership. On the other hand, as the contributions tend to be licensed under non-exclusive licenses, one could argue that there is no exclusive ownership, as the resulting digital works are non-rival and not artificially constrained. Indeed these works are considered "common goods" and are generally controlled by the community.

For a classification of ownership we refer to Elinor Ostrom's work, who received the Nobel prize in Economics in 2009[28] for her lifelong studies of common goods and commons governance models.

	Low rivalry (subtractability)	**High rivalry (subtractability)**
Hard excludability	Public goods	Common goods
Easy excludability	Club or toll goods	Private goods

Table 1 – Classification after E. Ostrom et al., 1994.

27 The term Commons-Based Peer Production (CBPP), introduced by Harvard Law School professor Yochai Benkler in his 2002 article "Coase's Penguin, or Linux and the Nature of the Firm", describes a new model of socioeconomic production in which large numbers of people work cooperatively, usually over the Internet: http://benkler.org/Pub.html.
28 https://en.wikipedia.org/wiki/Elinor_Ostrom.

4.2.1 Public domain vs intellectual property

In the various legal regimes that are lumped together under the term "Intellectual Property Rights", it is the state who grants an exclusive right, a monopoly right, to the solicitor. This exclusive right is considered to be temporary. Without it, the knowledge, ideas, creative work or mark would be in the so called public domain, that is to be used freely by all. Works in the public domain are those whose exclusive intellectual property rights have expired, have been forfeited, or are inapplicable. When exclusive rights expire, these rights return to the public domain (Boyle 2008).

4.3 Non-exclusive Public Licensing

Sharing creative works in a world dominated by exclusive copyright is not what lawmakers had in mind when devising the IPR legal system. In fact creative works – when the originality criteria are met – are by default covered with exclusive copyright protection, when made public. This implies that interested parties are required to negotiate a contract where the author(s) grant(s) the desired rights, a process that adds considerable complexity (and opportunity costs) to online collaboration. In the coming of age of the Internet Age, Knowledge Society, or Network Society, some did not consider this a socially desirable situation and public copyright licenses were designed to radically simplify this process. A non-exclusive or public license is one that conveys the basic rights to the general public so that effectively all can use them under equal rights.

It was software developer Richard Stallman[29], founder of the GNU project who defined these basic rights in the case of software as the four freedoms[30]: 1) to use it for any purpose; 2) to modify and adapt it to one's needs; 3) to share copies with one's neighbours, and 4) to distribute modified versions.

When in the 1980s Stallman devised the GNU General Public License (GPL) he referred to copyright law's exclusive rights assigned to the author, who subsequently conveys the four freedoms to the users. So effectively he flipped the "all rights reserved", and called it "all rights reversed". Additionally he included the so called *copyleft* condition that derivative works were to be published under the same license (in his case, the GPL). This historic license (and its subsequent versions) is still the most used free software license. The term "Open Source Software" highlights the open development model that is typically practised in these software communities.

The success of the open development model as demonstrated by the Free Software Movement inspired its physical version: Open Source Hardware, or Free Hardware Design. It advocates "the public provision of hardware design documentation" (Greenbaum 2013, p.257) and it follows the legal model of copyright-based public licenses (De Filippi et al. 2015). The community of practitioners has worked on its definition[31] and has formed the Open Source Hardware Association[32].

Scholars have elaborated some open hardware license models (Katz 2012), among them the TAPR Open Hardware License[33] (Ackermann 2009), developed under the auspices of the Tucson Amateur Packet Radio association (Greenbaum 2013), and the CERN Open Hardware Licence[34], developed at CERN (Ayass et al. 2012). These licenses allow the copyleft model on open source hardware design, despite the fact that software and hardware have different legal status. Indeed, software is

29 https://en.wikipedia.org/wiki/Richard_Stallman.
30 See the official Free Software Definition at the GNU project: https://www.gnu.org/philosophy/free-sw.html.
31 The definition of "Open Source Hardware" was collectively defined in 2010 and published at the Freedom Defined wiki: http://freedomdefined.org/OSHW.
32 Open Source Hardware Association: http://www.oshwa.org.
33 TAPR Open Hardware License: http://www.tapr.org/ohl.html.
34 CERN Open Hardware License: http://www.ohwr.org/projects/cernohl/wiki.

connected to the expression of an idea through a binary or alphanumeric code, while hardware refers to physical devices. From a legal perspective, this conceptual difference means a distinction under intellectual property regulation:

- *software* is protected by copyright and in some jurisdictions (such as US, Australia, and EU Member States) it does not have to be registered in order to come into existence;
- *hardware* is protected by patent law, just as new and inventive industrial products and processes (Daley 2016, p.32);
- *hardware design files* can easily be protected under copyright law, considering that copyright law protects "pictorial, graphic and sculptural works", which include "two-dimensional and three-dimensional works of fine, graphic, and applied art, photographs, prints and art reproductions, maps, globes, charts, diagrams, models, and technical drawings, including architectural plans".

Considering the design files needed for digital fabrication, the copyright holder has the exclusive right over the reproduction of the work, and any derivatives made of it. This should be a sufficiently strong basis for the open source licenses (Greenbaum 2013).

For determining the legal status of producing physical products based on a freely licensed digital blueprint (e.g., a CAD file), three main scenarios can be distinguished (Margoni 2013, p.240).

The first is when there is *identity* between the realised product and the digital blueprint. This means that the blueprint is complete and final, ready to be reproduced by a digital fabrication process such as 3D printing. Any intermediate act before printing is limited to possible cleanup of the CAD file – including checking for manufacturability and regulatory compliance –, conversion to the printing format, and configuration of settings. These acts can be considered marginal and non-creative, and therefore this can be considered an act of "reproduction" and not a derivative work. This can be compared to 2D printing of 2D files: they are also treated as reproduction. As long as the license permits reproduction, the 3D printing would be permitted.

A second scenario is when the produced item is *considerably different* from the original blueprint. This may be because the blueprint is not detailed enough (e.g., just a diagram or sketch) or because the second designer decides to modify the original blueprint. It must then be established whether the intellectual creation as present in the original blueprint is identifiable in the final result in a way that may constitute copyright infringement, or whether it is merely a product inspired by the original blueprint but that does not reproduce the original work in a way prohibited by copyright law.

If the latter applies – this would be the third case – the second designer would become the author of the *derivative work*, while the original blueprint's author retains control through his copyright in the original work. In this case of a derivative work, the original author's conditions (license) must be satisfied in order to avoid infringement of his rights. If the original author used a copyleft license, the second one must apply the same or a similar license, as detailed in the concrete license terms.

Given the complexity of each of the involved IPR regimes, we limit ourselves to a brief overview of some of the challenges that we can identify for sharing knowledge in the context of DiDIY:

- patents are time consuming, overly costly, and complex bureaucratic procedures for most people. Moreover, they are not automatically assigned as is the case with copyrights. For developers interested in sharing their hardware designs under a public license, patents are therefore – in most cases – not a good option (Ackermann 2009);
- copyright only covers the expression, not the technical idea or solution itself. However, most often copyright is the main legal framework used to assert rights that are licensed under a

public license. Therefore these licenses can, at best, protect the designs, but cannot avoid the privatisation of differently shaped objects that derive from the same design, even if the license used is a copyleft one;

- copyright-based hardware licenses can be considered applicable to the resulting physical objects when the digital blueprint is identical or identifiable in the resulting object. This is of particular relevance for digital fabrication technologies, such as 3D printing, as these allow people to produce almost exact copies of a digital blueprint;
- when sharing hardware designs and in particular when people engage in the manufacturing and distribution of hardware one should be sure no patents (owned by external parties) exist, or appropriate patent licenses should be in place. Discovering patents is however a complex endeavour, so much that some call it a legal minefield, where one often cannot be sure whether a patent exists and potential patent claims can arise later in the process, in particular when a project proves to be successful;
- patent applications require there is no "prior art" and to be sure there is enough novelty in the patent application. Different countries hold different standards of what "enough novelty" is. Looking on it from an other angle, we can appreciate that the existence of prior art can be a practical way to avoid patent registrations. Publishing a technical solution in an open access web portal is called Defensive Publication[35] and aims at creating publicly available prior art, thereby at least theoretically preemptying the possibility to acquire patents over that idea. However, often enough patent offices do not take sufficient time to study the existing prior art and patents maybe granted even if the idea or solution has already been published before. In those cases the public may request to revoke such patent, again a time consuming and costly task. While defensive publication through public disclosure may be good to prevent others from preventing an inventions, unfortunately smart patent attorneys often find ways to "route around" it. They claim novelty in some arbitrary add-on innovation and then try to make the scope of their patent as broad as possible thereby prohibiting incremental innovations by yourself or others;
- patent pools are another way that would be to used: everyone who wants to benefit from a patent is required to join the pool, and thereby is required to put all of their patents in the pool as well. Around the GNU/Linux ecosystem many patents are donated to such a pool, called the Open Invention Network[36]. In 2013 Google presented the Open Patent Non-Assert Pledge, that allows patent holders to let free or open source software projects freely use patents they own[37],[38]. It is used to protect the Android ecosystem and contains more than 200 patents at the day of writing[39].

4.4 3D printing of exclusively protected products and exemptions

Intellectual property law includes patents, design rights, copyrights, and trademarks. All of these ranges are vulnerable to infringements caused by DiDIY activities. As DiDIY refers in particular to the socio-technological phenomenon of digital fabrication and Internet of Things, we can observe the growing accessibility of related knowledge and data through open online communities[40]. This circumstance represents an interesting interplay between the 3D printing model itself, and Computer

35 See for an introduction: https://en.wikipedia.org/wiki/Defensive_publication.
36 About the OIN: https://www.openinventionnetwork.com/about-us.
37 https://www.google.com/patents/licensing.
38 https://www.eff.org/deeplinks/2013/03/google-makes-open-patent-non-assertion-pledge.
39 http://www.google.com/patents/opnpledge/patents.

Aided Design (CAD). In the specific area of DiDIY investigating the reaction of intellectual property law could represent a different aspect of how the evolution of new technologies is impacting this area.

DiDIY-related technologies and social practices enable the low-cost prototyping and manufacturing of physical artefacts from digital specifications. These tools and practices are emerging as effective amplifiers for the creativity and the skills of individuals, who can affordably develop "digitally self-made" objects, including such diverse options as extreme customisation ("unique-by-design" objects designed by 3D modelling software and generated by digital fabrication tools) and context-aware, networked interactivity ("smart" objects that can sense and respond to their environments).

This point is full of legal significance and it seems the core of our discussion because it contains in itself multiple legal perspectives. On the one hand, it represents the spread of the production system. Indeed, it is fragmented among a very wide audience of users that are at the same time producers and consumers of their final self-made goods (Dolinksy 2014, p.595). On the other hand, the hybridisation of intellectual property discipline could be problematic (Assay 2016). For instance, 3D printers could be subjected to patent law, Arduino boards to open source discipline (De Filippi 2015, pp.48 ss.), files to copyright law.

In the US legal debate, some scholars claim to extend First Amendment protection to DiDIY, especially to 3D printing. As it is well known, the First Amendment clause[41] is deeply involved in protecting freedom of speech and press in business activities[42] around new technologies. In this sense, some scholars argue on such an extension of First Amendment freedom because 3D printing would manifest creativity and freedom of speech. Indeed, "3D printing has transformed how we had traditionally understood "printing": printing now includes not only disseminating ideas, but also manufacturing objects" (Tran 2016). Other scholars respond that according to Article No. 27 of TRIPS, introducing new technology is a neutral occurrence under intellectual property law (Galli et al. 2015). Furthermore, 3D printing was not imaginable in 1791, when the First Amendment was adopted.

Conversely, fair use could provide a fair balance between the interests underlying the intellectual property model and DiDIY development. This is an exemption established by US copyright law for purposes such as criticism, comment, news reporting, teaching scholarship, or research. According to Rule 17 U. S. C. § 107, fair use allows third parties using protected works even without the author's permission, if four conditions are simultaneously observed: (1) the purpose and character of the use, including whether such use is of a commercial nature or is for non-profit educational purposes; (2) the nature of the protected work; (3) the amount and substantiality of the portion used in relation to the protected work as a whole; and (4) the effect of the use upon the potential market for or value of the protected work. This rule followed the strict dichotomy between copyright and patent law (Asay 2016), (Moffat 2014). However, over the years, scholars argued that patent law would benefit by a fair use defense (O'Rourke 2009), (Strandburg 2011) similar to what copyright law provides, especially given the so-called hybridisation between patent and copyright (Asay 2016, p.83 ss.). According to this point of view, "providing for a fair use defense to patent infringement

40 See for example this database of more than ten thousand 3D scans of physical objects: http://www.didiy.eu/blogs/large-dataset-objects-shows-relevance-didiy-project.

41 "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances".

42 M. Tushnet, Reflections On The First Amendment And The Information Economy, 127 Harv. L. Rev. 2233 (2014), 2249. E. Volokh, Freedom for the Press As an Industry, or for the Press As A Technology? From the Framing to Today, 160 U. PA. L. REV. 459, (2012), 459-540. E. Lee, Technological Fair Use, 83 S. Cal. L. Rev. 797 (2010), 813.

could allow patent law to respond more flexibly to a variety of scenarios where patent law as currently applied often results in excessively harsh effects on users of patented inventions" (Asay 2016, p.83), (Strandburg 2011, p.202).

Let us hypothesise a specific extension of fair use under patent law, connected to the expansion of DiDIY practices, since DiDIY is transforming the production of material goods following what has already happened with intangible, or informational goods, such as the fragmentation of production and the transformation of consumers/users into manufacturers/producers.

Courts have distinguished the purpose and the character of fair use into two separate inquiries: "whether the use is commercial or non-commercial, and whether the use is transformative" (Dolinsky 2014, p.619). In the first case, since the Sony v. Betamax case[43], the US Supreme Court stated that non-commercial use will constitute fair use (Dolinsky 2014, p.620) unless there is "proof either that the particular use is harmful, or that if it should become widespread, it would adversely affect the potential market for the copyrighted work". On the other hand, on the concept of transformative use, the US Supreme Court stated that it refers to "add something new, with a further purpose or different character, altering the first with new expression, meaning, or message"[44].

Regarding the nature of protected works, courts explored this issue through the analysis of two issues, precisely whether the work is creative or non-creative (Dolinsky 2014, p.623). In this case, the Ninth Circuit Court affirmed that a creative work is "closer to the core of intended copyright protection than are mere fact-based works"[45], and then "more likely to be covered by fair use" than a non-creative one. The second issue is about the publication of the work, because published works "are more likely to qualify as fair use because the first appearance of the artist's expression has already occurred"[46]. Concerning the amount of the work used, the Ninth Circuit Court affirmed that "the extent of permissible copying varies with the purpose and character of the use", then remaining very vague on this point. Relating to the effect of the use on the market, the US Supreme Court affirmed that this factor covers "not only the extent of market harm caused by the particular actions of the alleged infringer, but also whether unrestricted and wide-spread conduct of the sort engaged in by the defendant […] would result in a substantially adverse impact on the potential market for the original"[47]. Analysing the specific characteristics pertaining to DiDIY, the US fair use rule seems applicable to it.

According to EU law, and consequently the legal systems of EU Member States, DiDIY products made with 3D printers, and digital fabrication in general, should be subject to patent protection according to Articles 27-31 of TRIPs (Trade Related Aspects of Intellectual Property Rights) Agreement and Article 64 of the European Patent Convention.

These articles prohibit use of a patented product by third parties from producing, using, putting into commerce, or selling, or importing for these purposes. Therefore, in this specific context, the patentee is given any form of legal protection to go against any act that will take advantage of it, regardless of the quality of the product or specific added features, because according to the above mentioned legislation these activities are considered product counterfeiting (Galli et al. 2015).

However, EU laws allow 3D printing use for "domestic" production, excluding commercial, professional, or economic activities. In this case, DiDIY use of digital fabrication in a perspective of personal limited use is permissible, and the law makes no distinction of any kind. This exception

43 Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 454 (1984).
44 510 U.S. 569, LUTHER R. CAMPBELL AKA LUKE SKYYWALKER, ET AL., PETITIONERS v. ACUFF-ROSE MUSIC, INC.
45 A&M Records v. Napster, Inc., 239 F.3d 1004, 1118 (9th Cir. 2001).
46 Kelly v. Arriba Soft Corp., 336 F.3d 811, (9th Cir. 2003).
47 Campbell v. Acuff-Rose Music, 510 U.S. 569, 586-87 (1994); K. Dolinsky, at 624.

applies to any use of a private or personal nature, in good or bad faith. Actually, this exception is highly restrictive and "cuts off" shared use, albeit non-profit[48].

Some scholars have researched the case for UK law and have listed various exemptions applicable to non-commercial, private use (Bradshaw et al. 2010), then publishing an update in 2013 after several legal changes in the UK had taken place (Bradshaw 2013), in particular in the area of copyright and design rights. "Under UK and European law, there are some interesting implications for the use of 3D printers; for instance, purely private use of a 3D printer will not infringe design rights, but often would infringe the copyright of more artistic objects. Furthermore, it will in many cases be possible to print even on a commercial basis items such as spare parts and accessories, because of the exemptions in law intended to preserve a market for such items, or because very functional designs will not fall within either copyright or design right protection.".

According to Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, the exceptions and limitations provided for in Article No. 5, paragraphs 1, 2, 3 and 4 shall only be applied in certain special cases which do not conflict with a normal exploitation of the work or other subject-matter and do not unreasonably prejudice the legitimate interests of the rightholder. Such discipline remains the three-step test provided by Article 13 of TRIPs and Article 9.2 of the Berne Convention of 1986 for the Protection of Literary and Artistic Works.

How could these rules be interpreted in a less restrictive and stifling way in favour of a DiDIY environment? For example, in Italian Law, according to the principle of equality, established by Article No. 3 of the Constitution, equivalent situations should be treated accordingly (Galli et al. 2015). Article No. 68 of the Industrial Property Code limits the private use exception of patent-protected material only to cases where such use is economically irrelevant, or to cases where the individual does not make use of specific resources provided by third parties. Therefore, the realisation of the patent-protected product in the private and non-commercial sector through 3D printing is considered unlawful only when makers massively reproduce the project and the corresponding digital files for this purpose.

Even in the field of experimental research, exceptions to patent protection in EU and Italian legislation are more restricted than US legislation on fair use. For scientific and educational use, copyright protection exemption is granted only for non-commercial purposes according to Whereas No. 42 of the Directive 2001/29/EC and Articles 6.2 letter b) and Article 9 letter b) of the Directive 96/9/EC. In contrast, in Italian patent law, Article No. 68 of the Code of Industrial Property, private and non-commercial purposes are alternative, therefore the research and educational use exemption is wider (Galli et al. 2015). Furthermore, it should be considered that patent protection relates to the specific technical solution adopted, while copyright law protects the expressive content of a creative work. This distinction is crucial in the field of spare part production in a private context, especially in those of small dimensions pertaining to a bigger and more complex product. Scholars argue that the DiDIY production of these replacement parts with 3D printing systems should be permissible under Article No. 241 of the Code of Industrial Property (Galli et al. 2015), that is the implementation of Article 14 of the Directive 98/71/EC. Indeed, this use of DiDIY technologies could contribute to liberalising the spare parts market. The same scholars note that in order to prevent counterfeiting, this exception must be strictly applied to single parts and not to the production of standard components that could be involved in product reassembly, such as a remake of the original product.

48 C. Galli, A. Contini, op cit, p.51.

On this point Article No. 4 of Directive 98/71/CE (Implemented in Italy by art. 27 of Legislative Decree no. 95/2001) states that "whereas for this reason Member States should in the meantime maintain in force any provisions in conformity with the Treaty relating to the use of the design of a component part used for the purpose of the repair of a complex product to restore its original appearance, or, if they introduce any new provisions relating to such use, the purpose of these provisions should be only to liberalise the market in such parts.". According to the above mentioned scholars, this reform could take place only through the imposition on national legislators of exclusive rights to design and/or prototype of the element and not for other reasons (Galli et al. 2015, p.59). Consequently, if the object of the patented invention is the component, the counterfeiting of the patent is accomplished when the unauthorised reproduction imitates the component itself or its characteristics (Daly 2016, p.42), with no repair clause that could establish a limit in respect of the holder's rights, even if the reproduction is visible and detectable (Galli et al. 2015, p.59). From the amateur operator's perspective as in a DiDIY environment, this is a very restrictive regulation.

However, in the specific field of 3D printing, in case of design the aforementioned art. 241 of the Italian Industrial Property Code could represent an exception because it protects the legality of the creation of components of complex products, such as prototypes. An investigation should be made about who could benefit from the repair clause guarantees, and specifically, under the enforcement perspective, who should carry the burden of proof regarding the actual destination of the component parts if it is not intended to be integrated with the product itself (Galli et al. 2015, p.59). In this regard, Directive 98/71/CE ratio is to avoid forcing users to buy the original parts whenever the user needs to repair his or her object. However, such a ratio accomplishes the sense at the time when "the product requires the presence of a plurality of identical elements between them, which together contribute to the overall aesthetic appearance of the product complex" (Galli et al. 2015, p.60).

4.5 Internet of Things and privacy and anonymity

The Internet of Things (IoT) concerns the infrastructure in which many sensors are designed to record, process, store data locally or interacting with each other both in the medium range, through the use of radio frequency technologies (e.g., RFId, bluetooth, etc) and an electronic communications network. The devices involved are not only traditional computers or smartphones, but also dailylife objects ("things"), such as wearable, home automation, georeferencing, and assisted navigation objects. Indeed, the IoT refers to a further development of the Internet resulting from the physical objects networking. These objects that may be equipped with a unique identifier. e.g., a serial number, recognisable even by radio frequency. But the identification of these objects could also be done without resorting to radio labels, but by combining sensors and automatic recognition procedures (e.g., the recognition of a barcode carried out with a mobile phone connected to the Internet (Iaselli 2015, p.5). However, there is no universal definition of IoT (Rose, Eldridge, Chapin 2015, p.1).

4.5.1 Control of personal data

Internet of Things devices could present difficult issues because their sensors may capture a lot of information about people's identity, tastes, intention, behaviour. Then, all these pieces of information are filtered through "Big Data" analytics, drawing a revealing portrait of single persons habits, personalities and choices (Peppet 2014, p.89). Personal data could be spread in a wide range of sensitive area. For example:

- human devices attached or inside the human body: this refers to devices (wearables and ingestibles) monitoring and maintaining human health and wellness, disease management,

increased fitness, higher productivity; this is probably the most sensitive issue as it concerns the most intimate aspects of personal life;

- home buildings, where people live, especially home controllers and security systems;
- retail environments, i.e., areas open to the public where consumers engage in commerce, such as banks, malls, restaurants and anywhere consumers can buy products or products could be stored;
- office spaces, where employees and knowledge workers work;
- factories and other places where work is standardized with repetitive routines, such as hospitals and farms, where IoT can optimise equipment use and inventory;
- workplaces such as mines and construction sites, where IoT can improve predictive maintenance, health and safety issues;
- vehicles systems, such as cars, trucks, ships, aircraft, and trains;
- cities and urban environments, where IoT can improve public spaces and infrastructure in urban settings with adaptive traffic control, smart meters, environmental monitoring, resource management;
- outside uses include railroad tracks, autonomous vehicles (outside urban locations), and flight navigation with the check of real-time routing, connected navigation, shipment tracking (Manyika, Chui, Bisson, Woetzel, Dobbs, Bughin, Aharon 2015).

In this sense, the IoT raises multiple difficult questions. "Who owns the data these sensors generate? How can such data be used? Are such devices, and the data they produce, secure? And are Digital DIY producers and consumers aware of the legal implications that such data create – such as the possible use of such data by an adversary in court, an insurance company when denying a claim, an employer determining whether to hire, or a bank extending credit?" (Peppet 2014).

According to scholars, "the Internet of Things is redefining the debate about privacy issues, as many implementations can dramatically change the ways personal data is collected, analysed, used, and protected (Rose, Eldridge, Chapin 2015, p.2).

These questions are more relevant if a non-professional DiDIY maker is involved in an IoT project, since a hobbyist could not have the whole and proper legal competence on privacy protection issues.

4.5.2 Regulation issues

Regulating the IoT represents a strong challenge because the range of legal, regulatory and rights issues associated to it is broad. IoT devices create new legal and policy challenges that did not previously exist, and they amplify many challenges that already exist (Rose, Eldridge, Chapin 2015, p.39). Indeed, the legal implications associated to the IoT are wide and "include claims associated with product liability when sensors fail, intellectual property ownership and data licensing rights, and consumer discrimination" (Mcmeley 2014, p.71).

In the United States of America, the Federal Trade Commission (FTC), stated that: "The Commission staff recognizes that this industry is in its relatively early stages. Staff does not believe that the privacy and security risks, though real, need to be addressed through IoT-specific legislation at this time. Staff agrees with those commenters who stated that there is great potential for innovation in this area, and that legislation aimed specifically at the IoT at this stage would be premature. Staff also agrees that development of self-regulatory programs designed for particular industries would be helpful as a means to encourage the adoption of privacy- and security-sensitive practices. However, while IoT specific-legislation is not needed, the workshop provided further

evidence that Congress should enact general data security legislation. As noted above, there was wide agreement among workshop participants about the importance of securing Internet-enabled devices, with some participants stating that many devices now available in the market are not reasonably secure, posing risks to the information that they collect and transmit and also to information on consumers' networks or even to others on the Internet. These problems highlight the need for substantive data security and breach notification legislation at the federal level. The Commission has continued to recommend that Congress enact strong, flexible, and technology-neutral legislation to strengthen the Commission's existing data security enforcement tools and require companies to notify consumers when there is a security breach. Reasonable and appropriate security practices are critical to addressing the problem of data breaches and protecting consumers from identity theft and other harms. Notifying consumers of breaches after they occur helps consumers protect themselves from any harm that is likely to be caused by the misuse of their data. These principles apply equally to the IoT ecosystem. We emphasize that general technology-neutral data security legislation should protect against unauthorized access to both personal information and device functionality itself. The security risks associated with IoT devices, which are often not limited to the compromise of personal information but also implicate broader health and safety concerns, illustrate the importance of these protections. For example, if a pacemaker is not properly secured, the concern is not merely that health information could be compromised, but also that a person wearing it could be seriously harmed. Similarly, a criminal who hacks into a car's network could cause a car crash. Accordingly, general data security legislation should address risks to both personal information and device functionality (…)" (FTC 2015, p.48-49).

On this side of the Atlantic Ocean, the EU does not establish specific regulations in the IoT area, however on 31 May 2016, the Committee of Legal Affairs of the European Parliament published a "Draft report with recommendations to the Commission on Civil Law Rules on Robotics. (2015/2103(INL))".

This is a proposal to regulate the new area of "artificial intelligence". Indeed, it does not refer specifically to the IoT, but the ethical statements and liability proposals could be extended to the IoT area. For instance, as pointed out in the Draft Report itself: "G. whereas many basic questions of data protection have already become the subject of consideration in the general contexts of the Internet and e-commerce, but whereas further aspects of data ownership and the protection of personal data and privacy might still need to be addressed, given that applications and appliances will communicate with each other and with databases without humans intervening or possibly without their even being aware of what is going on; H. whereas the "soft impacts" on human dignity may be difficult to estimate, but will still need to be considered if and when robots replace human care and companionship, and whereas questions of human dignity also can arise in the context of "repairing" or enhancing human beings; I. whereas ultimately there is a possibility that within the space of a few decades AI could surpass human intellectual capacity in a manner which, if not prepared for, could pose a challenge to humanity's capacity to control its own creation and, consequently, perhaps also to its capacity to be in charge of its own destiny and to ensure the survival of the species.".

In what kind of role could the DiDIY practitioner be involved? According to many scholars, the collection of personal data is one of the most questionable issues of the IoT. In fact collected data can be used for discriminatory purposes based on gender, race, economic status or health of the persons to whom the data relates. However, a greater spread and involvement of DiDIY makers in this area could represent a strong shield against discrimination, through the spread of opportunities in the market.

4.5.3 Anonymisation

In this area, the main issue is related to IoT consumers' protection. It would seem that IoT products have become an inseparable mixture of hardware, software and service. Despite legal attempts to distinguish the different elements, this has become untenable. This convergence has, we would argue, implications for the applicability of consumer protection and privacy laws (Noto La Diega, Walden 2016).

Anonymisation represents a technical challenge, because IoT sensor data are particularly difficult to de-identify or anonymise. The sensors in IoT devices often have entirely unique "fingerprints" – each digital camera, for example, has its own signature imperfections and irregularities (Peppet 2014). However, scholars qualify this technical challenge "simple", because many IoT products have not been engineered to protect data security. These devices are often created by consumer-goods manufacturers, not computer software or hardware firms. As a result, data security may not be top priority for current IoT manufacturers. In addition, the small form factor and low power and computational capacity of many of these IoT devices make adding encryption or other security measures difficult (Peppet 2014).

Under a DiDIY perspective, it could be useful to deliver a disclosure about privacy and anonymisation that specifies the tools used for analysing the personal data collected and inform the final user (also for free consumers such as the maker's friends or relatives) about any data transferred to third parties for other purposes. It could be comparable to the "cookies policy disclaimer" that every content producer, professional or non-professional, must publish on his or her website.

The final user should be put in a position to refuse the use of the product with similar characteristics (Iaselli 2015). The IoT has to be seen always as a possibility, but not as an imposition. Like it we must consider the additional safety risks caused, specifically, by communication operations to third parties, misuse and loss of information handled, especially of the volumes and types of data, as well as use of the extensive use of the radio interfaces, structurally particularly vulnerable (Iaselli 2015).

As with all new technologies also for IoT devices the principles of transparency and privacy by design are to be applied and required by default in the forthcoming European regulations. Indeed, The principle of transparency requires that the information provided to the public is easily accessible and easy to understand and that a simple and clear language is used. Even for the IoT personal data must be processed lawfully, fairly, transparent and the controller must implement transparent and easily accessible policies and with regard to the processing of personal data and purpose the exercise of the user's rights (Iaselli 2015).

4.6 DiDIY Drones

4.6.1 What are drones?

A drone is an automated aircraft without pilots on board. Hence drones are also called Unmanned Aerial Vehicles (UAV) or Unmanned Airline Systems (UAS). Two types of drones have been developed until now:

- unmanned drones, that are automatically programmed and are independent because they are not piloted, not even remotely;
- Remotely Piloted Aviation Systems (RPAS), that are controlled by humans remotely. According to the current EU regulations, only RPAS are authorised for use in EU airspace.

Drones could be used for several reasons, one of the most important being warfare. Here only civilian uses are considered. Civil drones can be used in many different ways, for commercial

reasons such as good deliveries, photographic services, farm activities; for security issues such as inspections in industrial sites or dangerous situations such as fires, earthquakes, landslides, floods or in criminal investigations or safety checking, and so on. Indeed, drones could help to save health and human lives in threatening situations. Drones are then useful, but their use, even if not extensive, could cause problems of air traffic security, especially if they are used in areas close to airports or other sensitive spaces. Moreover, they could induce severe privacy, liability, trespass issues.

One of the larger areas of application of DiDIY methods is the drone environment, since DiDIY allows people with distinct technical skills to prototype their ideas and their projects before implementing them on a large scale.

4.6.2 Comparative perspective: the US overview

In the US the leading actor in this area of innovation, the Federal Aviation Administration (FAA), is involved in delivering a new set of rules on its Congressional mandate to integrate civilian drones into the National Airspace System (Perritt, Sprague 2015, p.675). The FAA distinguishes between non-professional makers, that make homebuilt aircraft, and those actors that use drones in commercial activities. These two groups are not always distinct. For example, a delivery professional can use a quadcopter made by him or herself in his or her commercial activities, or a farmer can use a similar device for spraying pesticide on his or her crop fields.

For the non-professional, non-commercial use ("Fly for Fun"[49]) there is a requirement for self-registration for drones weighing between 0.55 and 55 pounds (costing 5 US$ for a 3 years period). A registration number generated in the process must be duefully labelled on the device. Very small aircraft weighing less than 0.55 pounds do not require registration under this rule[50]. "For registration 60-120 days before contemplated completion of assembly. Before granting an airworthiness certificate, the FAA inspects amateur-built aircraft, including "an onsite, visual, general airworthiness certification inspection of the aircraft", and recommends involvement of designated airworthiness representatives (DAR's) before the inspection occurs. The inspection may require some disassembly. The FAA inspection includes review of inspections by certificated mechanics or other builders/commercial assistance providers, builders' construction log entries, logbooks and maintenance covering the aircraft, engine, and propeller or rotor blade(s), and Experimental Aircraft Association (EAA) technical counselors' visit report card Builders often must provide photographs documenting construction details. The inspection and records review substantiates sound workmanship methods, techniques, and practices."(Perritt, Plawinski 2016, p.8-9).

New rules for non-hobbyist drone pilots were published on 21 June 2016. They concern a broad spectrum of commercial uses for drones weighing less than 55 pounds. Even if they do not pertain to amateur use, they could provide an example of the balance between safety and drone use, even if a commercial one. Professional use of drones weighing less than 55 pounds ("Fly for Work/Business"[51]), apart from registration, also requires passing an exam at an FAA-approved knowledge centre and the vetting of the pilot by the Transportation Safety Administration (TSA).

4.6.3 Working on an EU legal framework

As in EU statutory provisions on drones has not yet been formalised, the American experience could be treated as an example. Under the EU perspective, safety is the main objective of aviation

49 https://www.faa.gov/uas/getting_started/fly_for_fun.
50 FAA examples of drones that do not require registration:
https://www.faa.gov/uas/getting_started/fly_for_fun/media/UAS_Weights_Registration.pdf.
51 https://www.faa.gov/uas/getting_started/fly_for_work_business.

regulation and the integration of RPAS will be done according to the principle that all operations will have an equivalent level of safety in comparison to regular, manned, aviation"[52]. Then, the Regulation (EC) No 216/2008[53] mandates the European Aviation Safety Authority (EASA) to regulate both UAS and RPAS, when used for civil applications and with an operating mass of 150 Kg or more. Law drafting is in progress and the EASA published a precise timetable on this issue[54]. However, EASA states that toys, such as quadcopters, capable of flying but not equipped with an internal combustion engine, are subject to Directive 2009/48/EC on the safety of toys.

According to EASA guidelines, the new harmonised regulation has to establish that drone operations (i) must be compatible with ICAO standards, (ii) respect the Charter of Fundamental Rights of the European Union, especially the respect for the right to private and family life, and the protection of personal data, (iii) ensure security, that means the prohibition of using drones as weapons for criminal or terrorist scopes, and (iv) guarantee third party liability and, consequently, insurance[55].

Experts and policymakers are evaluating what kind impact machines such as drones and artificial intelligence devices have on the protection of the privacy of individuals. On the other hand, another question necessary to solve is about what kind of insurance is necessary to provide for the drone and AI robot activities.

While at the EU level there are no shared legal solutions, some Member States have approved some regulations.

4.6.4 National regulations

Newspapers reported a huge number of serious accidents involving drones worldwide (Michaelides-Mateou 2015). Because of the spread of drones, both for commercial and non-commercial use, national legislators are following the trend to consider drones "aircraft" and to impose aviation rules to them, regardless of their type of use.

Waiting for a harmonised EU regulation, some EU Member States have started to fill the lack of law in different ways. Here, we focus on five countries: Italy, Germany, Netherlands, Sweden, and the United Kingdom.

Italy

In Italy, the "Ente Nazionale dell'Aviazione Civile" (National Civil Aviation Agency, ENAC) published its first regulation in 2013; it entered into force in 2014. This regulation establishes a very complicated set of technical and legal rules, that harnesses the initiatives of individuals. The intended aim of this regulation is the attempt to deter the spread of the drones. Later in 2014 and in 2015 there were some corrections to the legislation in question, placing distinctions between UAV and RPAS, preparing specific concrete concepts, in reference to privacy and liability general rules[56].

Germany

52 www.easa.europe.eu.
53 https://www.easa.europa.eu/document-library/regulations/regulation-ec-no-2162008.
54 EASA, Introduction of a regulatory framework for the operation of unmanned aircraft, 2015, p.30: https://www.easa.europa.eu/system/files/dfu/Introduction%20of%20a%20regulatory%20framework%20for%20the%20operation%20of%20unmanned%20aircraft.pdf.
55 https://www.easa.europa.eu/unmanned-aircraft-systems-uas-and-remotely-piloted-aircraft-systems-rpas.
56 www.enav.gov.it.

In Germany, private use of drones is prohibited at a height of over 100 meters and out of sight of the user, over special places such as industrial plants, prisons, military facilities, power plants, freeways, and railways. The commercial use of drones requires a permission, and the pilot's knowledge of aviation law shall be tested in an examination. The permission is issued by the German Federal Aviation Authority. The Federal Office for Transport and Mobility affirmed that they are working on changes in the currently relevant legislation[57].

Netherlands

The Dutch rules on drones affirm that the drone must always be visible to the pilot. The recreational or private use of drones follows the regulation applicable to flying. Professional users need a specific permit for this activity. They also must have a proof of registration in the aircraft register, a special Certificate of Airworthiness, a RPAS Operator Certificate and the flight school must be registered as RPAS flight school, submitted to regular technical inspections[58].

Sweden

Sweden approved drone regulation in 2009. It is related to commercial use of drones and it establishes precise distinctions among categories of UAS and RPAS in a weight perspective. A two year permission is requested for using drones, under a formal declaration for beginning of commercial drone activities[59].

United Kingdom

In the United Kingdom the user of a RPAS needs a permission, delivered on a case by case basis. It is valid for one flight or for a period of up to 12 months. Applicants must demonstrate to have ensured sufficient safety measures, especially that the drone will not endanger people, property or aircraft. Frequent users, such as individuals or organisations, i.e., emergency services, that would like to conduct regular flights with their drone, however, need to submit an operating manual to the CAA for a permanent approval[60]. This also applies for non-commercial activities. However, if certain (location-based) limitations are adhered to, permission may not be needed. The UK CAA has published a code of conduct, the "Drone Code", to provide this category of users with guidance[61].

4.6.5 Some provisional conclusions

It seems that non-commercial, non-professional activities with typically small, lightweight UAS are hardly regulated in most jurisdictions. The EASA proposes a "harmless" subcategory for this, only subject to market regulations and local restrictions, but not imposing the heavier burden of pilot exams and the request of permissions.

From the point of view of data protection what is relevant are the various sensors and capturing devices that may be fitted onto the UAS (that is, high-resolution cameras and microphones, thermal imaging equipment, devices to intercept communications) and the subsequent collection and processing of personal data that this would constitute, sometimes against unsuspecting people taking into account the limited size of some of these devices (Iaselli 2015). Moreover, if the same

57 http://www.bmvi.de/SharedDocs/DE/Artikel/K/151108-drohnen.html.
58 https://www.ilent.nl/onderwerpen/transport/luchtvaart/dronevliegers.
59 http://www.transportstyrelsen.se/globalassets/global/luftfart/luftfartyg/the-swedish-uas-regulation-tsfs-2009-88.pdf.
60 http://www.caa.co.uk/Commercial-industry/Aircraft/Unmanned-aircraft/Guidance-on-operating-permissions-for-drones.
61 http://www.caa.co.uk/Consumers/Model-aircraft-and-drones/The-Dronecode.

drones were visible, it would be extremely difficult, if not impossible, to know who is watching, for what purpose, how and why for claiming proper rights. This specific issue could emerge regarding the person who is liable under tort law for incidents occurred because of the use of RPAS. Using a clearly visible identification number may remedy only part of this challenge, again because of the small size of some of these devices.

Regarding a possible future regulatory framework, none of the measures currently being discussed at EU level (General Regulation on Data Protection and Regulation of policing and justice, the directive on data protection in criminal matters) includes specific provisions relating to the processing of personal data performed by means of drones and to the consequent liability (Iaselli 2015).

4.7 Blockchain technologies for distributed applications

Blockchain is a recent technological platform that allows its users to store transactions in an immutable way in a distributed database. The concept, which was pioneered by the cryptocurrency called Bitcoin since 2009, combines a distributed network of users each of them having a copy of the complete set of transactions that have been performed up to date. By connecting the chain of transactions in blocks – hence the name "blockchain" – Bitcoin solved the problem of double spending of a digital currency. Furthermore its distributed architecture avoids the need of a "trusted third party" like a central bank or central registration authority. It is therefore also called a "trustless" architecture, as its transparent and distributed architecture enables one to trust even strangers. The avoidance of such intermediary is both offering unprecedented opportunities as well as challenges for it being difficult to impose external control.

While Bitcoin as cryptocurrency has caused legislators around the world to issue specific regulations on this innovative and challenging digital currency, what interests us here is the use of blockchain technology for distributed applications. Indeed over the last few years several blockchain-based platforms have emerged that allow people to build distributed applications of any kind, not just of a cryptocurrency. Ethereum may be one of the most advanced, which started in 2014, developing its platform to "Build Unstoppable Applications"[62]. We will briefly introduce the main concepts before discussing some of its opportunities and challenges in the context of DiDIY.

4.7.1 Smart Contracts

Through the introduction of Smart Contracts two or more users can agree to a set of terms and conditions in a digital contract that is written in computer code and is executed through the distributed network. The details of a Smart Contract are verified, or enforced automatically, thereby reducing its transaction costs. Such contracts can cover simple exchanges of goods and services between users, or increasingly complex arrangements of crowdfunding, or complete business models.

4.7.2 Decentralised Autonomous Organisations (DAO)

A Decentralised Autonomous Organisation (DAO), or Decentralised Collaborative Organisation (DCO), is an algorithmically-governed programme that, in using "trustless" decentralised computing, can serve as a way to formalise multilateral relationships or transactions outside of traditional legal architecture. In legal terms, a DAO is therefore a medium for two or more people to conclude agreements or otherwise associate with others in a predictable way (Szabo 1997). The fact that a DAO built on a blockchain operates itself in accordance with pre-defined rules and

62 Ethereum's slogan, see https://ethereum.org.

cryptographically secure architecture means that its users can reliably expect instructions which they broadcast to be consistently and securely executed.

According to Ethereum co-founder Vitalik Buterin, "Blockchains are not about bringing to the world any one particular ruleset, they're about creating the freedom to create a new mechanism with a new ruleset extremely quickly and pushing it out. They are Lego Mindstorms for building economic and social institutions." (Buterin 2015).

"These are essentially self-organised online commons. A DAO could use blockchain technology to give its members specified rights within the organisation, which could be managed and guaranteed by the blockchain. This set of rights, in turn, can be linked to the conventional legal system to make those rights legally cognisable"[63].

Slock.it, a pioneering company developing smart lock devices, is arguably the first to make this idea real, combining low-cost computing devices to run a personal node in the decentralised Ethereum network, from where people can control their physical assets, negotiated and controlled through blockchain applications, connecting sensors and actuators (Internet of Things) and managed as a democratic DAO[64].

Currently the state of development of these platforms is still experimental, where the underlying protocols and toolsets are still being developed and improved. This is both a competitive as a collaborative process. Competitive as many small companies are developing competing applications, large banks setting up their specialised departments etc. Collaborative in the sense that knowledge is shared, large part of the code is shared freely, and new applications emerge incorporating the innovations of predecessors. Regulators and governments have begun to take the technology seriously and are struggling to catch up (Walport 2016).

Some legal challenges that are already identified or can be expected in the near future are as follows:

- although blockchain technology is, at least in theory, more transparent than traditional exchange systems, in practice users have various options to obfuscate their identity (Reid, Harrigan 2011);
- blockchain technology adds to the IoT the self-governance of distributed applications that automatically execute smart contracts and code embedded in them; this may challenge consumer protection, telecom, IPR, contract law, fiscal and other regulations;
- the distributed architecture of blockchain technology assures its functioning without any form of central control; this ultimately may challenge the nation state in its ability to regulate the economy by means of traditional monetary policies in the case of cryptocurrencies (De Filippi 2014) and may challenge the ability to regulate society at large when distributed application platforms like Ethereum consolidate;
- blockchains are not just a new technology but more fundamentally are a new mode of governance that competes with other economic institutions of capitalism, namely firms, markets, networks, relational contracting and governments (Davidson 2016).

4.8 Pathogens and 3D printed guns

With the advance of low-cost digital fabrication, technology enables DiDIY to engage in producing complex products, including dangerous weapons and pathogens. People perceive these as a threat

63 David Bollier in his report on Distributed Networks and the Law: http://bollier.org/distributed-networks-and-law.
64 See the Slock.it website for more in depth information: https://slock.it.

and as the production of these dangerous artefacts is based on digital fabrication techniques, one can speak of *dangerous information*.

A famous case is the first 3D printed hand gun, called the Liberator. It can be downloaded from the Internet and printed on a low cost 3D printer. Apart from the risk of blowing in your hands it can be used one time only. A more sophisticated gun that can be CNC milled is the GhostGunner[65]. For an amount of about 1200 US$ one can buy a CNC machine that mills the holes in a unregistered gun part (available on the market) so accurately that amateurs are said to be able to produce their own semi-automatic weapon. An organisation called Defense Distributed[66] runs this project and distributes the CNC machines.

We can distinguish four categories of production or uses of potentially dangerous information (Tebbens, Fioretti 2015):

- the "mere" production and distribution/sharing of digital files containing the design of physical objects and necessary code and data;
- the actual fabrication of these objects using the digital information;
- the intentional usage of digitally fabricated objects to engage in unlawful activity, including objects that are not weapons at all (examples may be "innocuous" drones used for burglary, the Arduino-based Lock Breaker or, construction-industry power-tools self-made or modified, in ways impossible without DiDIY, just to break into a bank vault);
- the unintentional damage to oneself or other people or their possessions by using DiDIY-made (unregulated) objects.

There are serious debates about this topic[67], about whether this could mean the end of gun control. Whether it would make sense to regulate the use of dangerous information, and whether the dangers of dangerous information outweigh its potential positive effects, will be discussed at length in the forthcoming deliverable D6.2, "Report on ethical impact for regulation".

65 https://www.wired.com/2014/10/cody-wilson-ghost-gunner.
66 https://defdist.org.
67 See for example some debates on the DiDIY blog: http://www.didiy.eu/search/node/weapons.

5. Sharing Knowledge: solutions practised

As knowledge sharing is an essential aspect of the practice of DiDIY, we have studied the ways individuals, companies and communities deal with the legal challenges and obstacles to sharing knowledge. In this section we intend to present a practical overview of solutions practised, and discuss their strengths and weaknesses. First we present an overview of some of the main non-exclusive licenses for software, documentation and artwork, and hardware designs (the "Licensing guide"). We continue with an overview of some of the relevant online platforms where people share their designs and other works relevant for DiDIY. We discuss then the practises of protecting privacy and anonymity, and end with a brief overview of ways people deal with liability in this context.

5.1 Licensing Guide

Digital resources that are shared over the Internet typically use licenses that define under what conditions the resource is made available. As mentioned before, copyright conveys "All rights reserved" to the author of an original work. Standard licenses are arguably the most convenient and common way for the author to define the conditions of use of his/her work. When the license conveys all basic rights to the general public we can talk about a "non-exclusive" license, and when anyone can use the license it can be called a "public license". In this section we discuss the most common licenses, classified in different groups.

5.1.1 Copyleft vs. permissive

We can distinguish between "free", "open", and "closed", "non-free" or "proprietary" licenses. Within the first two groups we have "Copyleft" and "permissive" licensing options. Copyleft refers to the license condition that requires modified versions to be made available under the same or a similar license (such as the term "ShareAlike" in the Creative Commons licenses denotes). The lack of this condition makes a license "permissive" in that it permits modified versions to be made proprietary, even though authorship should always be attributed.

5.1.2 Free Licenses vs. open licenses

Free licenses aim at protecting the four freedoms over a work. Authors convey through such license the main four types of rights, that were originally defined for the case of free software but have been found applicable to many other domains as well. Following is the Free Software Definition, where Free Software is that which its author(s) have released granting the following four freedoms or rights over the corresponding work to any user:

- freedom 0: the right to use the work for any purpose;
- freedom 1: the right to study and adapt the work;
- freedom 2: the right to share copies with one's neighbour;
- freedom 3: the right to distribute modified versions[68].

The Free Software Foundation (FSF) keeps a list of free licenses with various classifications, and similarly do the Open Source Initiative[69] (OSI) and the Open Knowledge Foundation (OKFN). Creative Commons offers a set of licenses ranging from copyleft free licenses (CC BY-SA) to permissive free licenses (CC BY) to more restricted licenses that allow NonCommercial restrictions

68 Freedoms 1 and 3 require the source code to be accessible.
69 OSI license list: https://opensource.org/licenses.

or NonDerivative limitations. While OSI and OKFN consider "open licenses" to refer to generally the same license base as "free licenses", still many people consider the whole set of Creative Commons licenses to be open licenses as well, while CC licenses, as just mentioned, include several non-free licenses, excluding commercial usage or derivatives. To avoid confusion it is therefore recommended to consider free licenses those protecting a work with the four freedoms and making it a non-exclusive work. For that purpose the Freedom Defined[70] initiative was erected, which keeps a list of licenses that protect the four freedoms. The term "open license" denotes then the bigger realm including free licenses and those licenses that reserve some rights, such as the privilege to participate in commercial activity (such as CC BY-NC) or make derivative works (such as CC BY-ND).

5.1.3 FSF-approved "free software" licenses

The Free Software Foundation (FSF), the group that maintains the Free Software Definition, maintains a non-exhaustive list of Free Software licences at the GNU website[71]. The FSF is a nonprofit with a worldwide mission to promote computer user freedom and to defend the rights of all free software users[72] and is the legal host for the GNU project. Free software developers guarantee everyone equal rights to their programs; any user can study the source code, modify it, and share the program. By contrast, most software carries fine print that denies users these basic rights, leaving them susceptible to the whims of its owners and vulnerable to surveillance.

The FSF prefers copyleft (share-alike) Free Software licensing rather than permissive Free Software licensing for most purposes. Its list distinguishes between free software licenses that are compatible or incompatible with the FSF copyleft GNU General Public License.

5.1.4 OSI-approved "open source" licenses

The Open Source Initiative (OSI)[73] defines and maintains a list of approved open source licenses. OSI agrees with FSF on all widely used Free Software licenses, but differs from FSF list on some less frequently used licenses, that it approves against the Open Source Definition rather than the Free Software Definition.

5.1.5 Free Software licenses

License Name	Abbreviation	Author/Maintainer	First version	Type	Particularities
GNU General Public License[74]	GNU GPL	FSF	1985 / 1989	Copyleft	Patent grant; forbids the use of DRM
Lesser General Public License	GNU LGPL	FSF	1991	Weak copyleft	Designed for software libraries
GNU Affero General Public License[75]	GNU AGPL	FSF	2007	Copyleft	Requires modified version running in a network to be shared

70 Freedom Defined license list at http://freedomdefined.org/Licenses.
71 FSF Licensing list at https://www.gnu.org/licenses/license-list.html.
72 Free Software Foundation: http://www.fsf.org.
73 Open Source Initiative: https://opensource.org.
74 GNU GPL: https://gnu.org/licenses/gpl.html.
75 GNU AGPL: https://www.gnu.org/licenses/agpl.html.

License Name	Abbreviation	Author/Maintainer	First version	Type	Particularities
Apache License[76]	ASL	Apache Software Foundation	1995	Permissive	Patent grant
MIT[77]	MIT PL	Massachusetts Institute of Technology	1988	Permissive	For software and its documentation
Berkeley Software Distribution Licenses[78]	BSD Licenses	University of California/Public Domain	1999	Permissive	Different versions of the license have different clauses
Mozilla Public License[79]	MPL	Mozilla Foundation	1998	Partial	Especially used for Mozilla projects
European Union Public License[80]	EUPL	European Union	2007	Copyleft	For software and its documentation; in 22 EU languages

Table 2 – Free Software licenses.

The comparison of Free Software licenses is based on (Rosen 2004), the primary sources of these licenses and the Free Software license comparison in Wikipedia[81].

5.1.6 Documentation and cultural works licences

License Name	Abbreviation	Author/Maintainer	First version	Type	Particularities
GNU Free Documentation License[82]	GFDL	FSF	2000	Copyleft	
Creative Commons Attribution[83]	CC BY	Creative Commons Int'l	2004	permissive	
Creative Commons Attribution ShareAlike[84]	CC BY-SA	Creative Commons	2004	copyleft	

76 Apache Licenses: https://www.apache.org/licenses.
77 MIT PL: https://en.wikipedia.org/wiki/MIT_License.
78 BSD Licenses: https://en.wikipedia.org/wiki/BSD_licenses.
79 MPL: https://www.mozilla.org/en-US/MPL.
80 EUPL: https://joinup.ec.europa.eu/community/eupl/og_page/european-union-public-licence-eupl-v11.
81 https://en.wikipedia.org/wiki/Comparison_of_free_and_open-source_software_licenses.
82 https://www.gnu.org/copyleft/fdl.html.
83 https://creativecommons.org/licenses/by/4.0.

License Name	Abbreviation	Author/Maintainer	First version	Type	Particularities
		Int'l			
Creative Commons Attribution Non-Commercial[85]	CC BY-NC	Creative Commons Int'l	2004	Non-free	Commercial use is reserved to the author(s)
Creative Commons Attribution No-Derivatives[86]	CC BY-ND	Creative Commons Int'l	2004	Non-free	Distribution of modifications of the work is reserved to the author(s)
Creative Commons Zero[87]	CC0	Creative Commons Int'l	2009	Permissive/ public domain	Authors grant all possible rights to the public domain or wave them

Table 3 – Documentation and cultural works licences.

More licenses for sharing documentation and cultural works can be found at the FreedomDefined wiki[88].

5.1.7 Hardware designs

In 1997, Bruce Perens announced the "Open Hardware Certification Programme"[89] to certify computer devices that have made available documentation on their device components and device drivers. In later years the term "Open Source Hardware" has been coined to refer to hardware designs that are documented and licensed under a free license. It was argued that the openness of (physical) hardware is not directly related to the design files being released under free or open licenses. The term "open source" in relation to hardware was to signal that the sources of the hardware that can be built with them is "open". To further define the term Open Source Hardware, the community has been working on a consensus-based definition, which emerged during 2010-2011 as follows: "Open Source Hardware (OSHW) is a term for tangible artefacts – machines, devices, or other physical things – whose design has been released to the public in such a way that anyone can make, modify, distribute, and use those things". The full definition can be read at the Freedom Defined wiki[90]. This work was done during the Open Hardware Summit, a yearly event organised by the non-profit Open Source Hardware Association[91].

Richard Stallman introduced the term "Free Hardware Design" in 1999[92], referring to hardware designs that users are free to copy, modify and convert into physical hardware. Even though a minority of the community uses this term, it can be considered an important synonym for what was

84 https://creativecommons.org/licenses/by-sa/4.0.
85 https://creativecommons.org/licenses/by-nc/4.0.
86 https://creativecommons.org/licenses/by-nd/4.0.
87 https://creativecommons.org/publicdomain/zero/1.0/legalcode.
88 http://freedomdefined.org/Licenses.
89 A copy of the announcement can be retrieved from the Internet Archive: http://web.archive.org/web/19981212031618/http://www.openhardware.org.
90 http://freedomdefined.org/OSHW.
91 http://www.oshwa.org.
92 http://www.linuxtoday.com/infrastructure/1999062200505NWLF.

later called "Open Source Hardware". A more extensive discussion of Free Hardware Designs can be found on the GNU website[93].

In 2014 the OpenHardware.org website went offline and since the operations seem to have ceased.

License Name	Abbreviation	Author/Maintainer	First version	Type	Particularities
Tucson Amateur Packet Radio Open Hardware License[94]	TAPR OHL	TAPR	2007	Copyleft	Based in copyright, patents and any other intellectual property right
CERN Open Hardware License[95]	CERN OHL	CERN	2011	Copyleft	Based in copyright in the documentation; includes a patent license
Solderpad Hardware License[96]	SHL	Andrew Katz[97] / Solderpad	2012	Permissive	Based in the Apache Software License, including database and patent rights

Table 4 – Open Source / Free Hardware licences.

5.1.8 Hardware certifications

Given that licenses are mostly based in copyright, which can help protect the design files and documentation but the resulting products only partially, other solutions have been developed to ensure or indicate that products are truly "Open Source Hardware".

Marking the products with a trademark-protected product label or certification is a relatively straightforward and practical solution to this issue. The product label can only be used if certain conditions are met, as set by the owner of the trademark.

The OHANDA product label was the first of its kind in applying their protected trademark only to products that comply with the four freedoms and have their designs and documentation published under a free license. This label certifies that the hardware labelled with it, is published at the OHANDA website under an accepted free license[98].

In 2011 the Free Software Foundation started a certification programme called "Respects Your Freedoms" (RYF) to certify computer hardware[99] that has its designs and documentation published with a free license, is free from non-free software and backdoors, and allows users to install their (modified) software.

A more recent effort is the Open Source Hardware Certification programme that is being developed at the Open Source Hardware Association: it is similar as the original OHANDA initiative, and requires self-assessment and labelling[100].

93 https://www.gnu.org/philosophy/free-hardware-designs.en.html
94 http://www.tapr.org/ohl.html.
95 http://www.ohwr.org/projects/cernohl/wiki.
96 http://solderpad.org/licenses.
97 See Katz discussion of a modified version of the ASL in (Katz 2012).
98 OHANDA, the Open Source Hardware and Design Alliance: http://www.ohanda.org.
99 https://www.fsf.org/resources/hw/endorsement/respects-your-freedom.

5.2 Online Sharing Platforms

5.2.1 Software

Software is often a crucial component of DiDIY, and some of the main platforms used for sharing (free) software are also being used for the sharing of hardware designs. We present here a brief list without further details: GitHub[101], Sourceforge[102], GitLab[103], Savannah[104], Launchpad[105]. We encourage the reader to check out their details online.

5.2.2 Platforms for sharing hardware designs

There is a range of online platforms that allow people to share hardware designs. We have conducted a review of some of the main platforms that are particularly useful for the practise of DiDIY. The compared platforms allow users to register, upload and share files under certain conditions. The licensing options offered (to share one's works under) are relevant here. Furthermore platforms differ in the technical and social features they provide. Also the governance of the platform is of importance to align the interests of users with those of the maintainers of the platform. In the following two pages we present a table summarising the comparative, while more details, and a possibly more updated version can be found online[106].

100 OSHWA's version 1 of its certification programme: http://www.oshwa.org/2015/09/19/open-source-hardware-certification-version-1.
101 https://github.com.
102 https://sourceforge.net.
103 https://gitlab.com.
104 https://savannah.nongnu.org.
105 https://launchpad.net.
106 FKI Wiki on Design Sharing Platforms: http://wiki.freeknowledge.eu/index.php/Design_Sharing_Platforms.

Online platforms for sharing designs															
Name	Slogan	Domain(s)	Ownership	Sustainability model	Software	Software license	Technical features						Encourage sharing		Comments
							formats	rendering	API	version history	friending	other features	licenses	reputation features	
OpenBuilds	Dream it - Build it - Share it	3D, electronics	OpenBuilds Part Store	Margins on parts sales	Unknown	Unknown	Sketchup, gCode, STL, dwg, obj, jpg, doc.., etc	No		No	follow	forums	CC	Ratings, likes, views, user profile	Share a part; OpenBuilds Store incl FairShare program
Youmagine	Share Your Imagination	3D	YouMagine 3D BV	?	Unknown	Unknown	STL, AMF, SCAD, JSCAD, OBJ, DAE, OFF, 3DS, PLY	yes		no	follow	collections, ideas, comments, direct message, QR print out	CC, GPL, LGPL, BSD	rate, favourite, # downloads, user profile	Partnership with Ultimaker
Open Hardware Repository	a place on the web for electronics designers at experimental physics facilities to collaborate on open hardware designs	Electronics	CERN	CBPP/community	Chili Project	GPL v2	any	no		yes (git / wiki)	no	per project mailing list, git repository, wiki, news, documents, issue tracker	CERN OHL, GPL, LGPL, TAPR OHL	user profile, activity statistics, highlighted projects	community encouraging freedom & openness in electronics
Fritzing	Electronics made easy	Electronics	University of Applied Science Potsdam	CBPP/Donations	Fritzing	GPLv3	Fritzing, Gerber, SVG, PDF, XML, Spice	Breadboard, Schematic, PCB, Code		no	no	Forum, Sharing, Autorouting	CC BY/BY-SA/BY-NC/BY-NC-SA	user profile	services for PCB production, parts, ...
Bld3r	A 3D Printing Social Network	3D	private	CBPP/Community	Bld3r	AGPL	Any file: upload / link / torrent	no		no	yes	printshelves (to print & printed), comments, wiki	free and NC licenses	user profile, ratings of user, objects, comments	Commons based community
Yeggi	Search engine for printable 3D models	3D	yeggi UG (Ltd. Germany)	Advertising	unknown	unknown	any	no		no	no	lists, tag notifications	any 3D model from the web	popularity	search engine
ThingTracker	A proposal on sharing designs and projects in the maker community.	3D, electronics, any thing	Gary Hodgson c.s.	CBPP	Specification on Github	no license specified	any file						any license		a distributed protocol for a thing network

Table 5 – Platforms for sharing hardware designs (first part).

Open Design Engine	Web portal to publish the entire design process for open source hardware projects	Electronics, 3D	Mach30 Foundation for Space development	CBPP/Donations	Redmine	GPLv2	any file	no		yes	no	Wiki, Forum, Roadmap, Gantt, Issue tracker, News	Clear distinction between Hardware/Software /Documentation licenses	user profile	Complete design process, OSHW only
Makerystreet	Stuff that a maker would find interesting	Electronics, 3D	Alex J V (OSHW maker)	Unknown	in Django at github	Apache2	any document, image or video (upload or link)	no		yes	yes	groups, assemblies, subassemblies, insights, forum, private/public projects	no license	userprofile, reviews, contribution stats	governance & licenses should be clarified
Libre3D	Libre3D Free & Open Source	3D	informal Community	CBPP	Libre3D Renderer	LGPL	SCAD, STL, PDF, images, Blender, Doc, XLS, ZIP, Videos	yes (SCAD, STL, videos)		no	no	contact, showcase	CC licenses, GPL, MIT, BSD, PD	user profile	strong relation w/ RepRap
Ohanda	4x Freedoms = Unlimited & Unconditional	Electronics, 3D	informal Community	CBPP/Donations	Unknown	-	HTML	no		no	no	no	any free license	producer page	trademark protection
Thingiverse	Digital Designs for Physical Objects	3D	MakerBot Industries, LLC	Sell MakerBot printers	Unknown	Unknown	stl, obj, thing, scad, amf, dae, 3ds, x3d, blend, ply, dxf, ai, svg, cdr, ps, eps, epsi, sch, brd	yes	public	no	follow	collections, customizer, apps, API	CC/GPL/LGPL/BSD	user profile, likes, made one, watch, remix	Shout out OR tag
DIYdrones	The leading community for personal UAVs	UAVs	Chris Anderson/3D Robotics	CBPP	Unknown	Unknown		no		no	yes	blog, forums, groups	CC BY	profile page	3D Robotics store integrated
Wevolver	Build Technology Together	3D, electronics	company	Sells supplies	Based on Python/Django	Older version under AGPL	any	no		no	yes	project teams, subassemblies, forking	any	network diagrams of contributor relations	unstructured license info
Instructables	DIY How To Make Instructions	electronics	Company Autodesk	freemium: pro membership + CBPP	unknown	unknown	any	no		no	follow	collections, collaboration, forums, groups, faqs	CC, GPL, APL,PD and none	user profile, favourites, featured, "I Made it"	
Hackster.io	Hackster is a community dedicated to learning	electronics, code, 3D	Hackster Inc.	CBPP	unknown	unknown		no		no	follow	components, build instructions, team	no license	user profile, followers, featured, replicated	

Table 5 – Platforms for sharing hardware designs (second part).

5.3 Practises to deal with liability

When sharing creative works there is no commercial transaction. Still authors can be held liable for ignorance or other lack of their "duty of care". Typically authors share their works under a free or open license, and the license has a section on "warranty and liability". In this section we briefly discuss some examples and their importance for sharing works in a responsible way.

Warranties and liability clauses could represent the core of the balance between the duty of care of makers and the protection of users that want to try new objects or prototypes produced in experimental way and freely shared at public disposal or in a community. It is a sensitive balance because it represents the innovation core of DiDIY.

In this issue, the main question is how to legally protect the position of each participant in this scenario. On the one hand, for example, the DiDIY maker needs to avoid defatigant and expensive litigation on experimental prototypes and, at the same time, he or she needs the public confrontation and feedback on the possible defects or mistakes in his or her project. On the other hand, the user should be warned about possible damages caused by a prototype or an innovative tool.

In this perspective writing specific and proper warranties and warning clauses is recommended for the maker who shares with other parts (people, interested parties, communities) his or her invention, object, prototypes, especially in case of experimental projects. Writing generic standard clauses is not recommended because users could not be aware of risks, danger and damages that could be caused by objects related to a high innovative environment such as DiDIY. Independent of this recommendation, the license terms of the listed licenses have disclaimers that state the files are provided "as is", without fitness for a particular purpose and only by accepting all risks, and a licensee is allowed to make use of the files in the first place according to the conditions placed in the license.

Warnings one could issue could include:

- the product/prototype shall be used only for the purpose/aim that the inventor/maker attributed to it;
- a specific warning about the improper use of the experimental or innovative object;
- a specific warning about the possible mistakes or defects in the design of the experimental or innovative object;
- a specific warning that the user can use the specific experimental object "as is" on "his or her own risk" (this is also included in a typical license);
- finally, subscribing a proper (collective) insurance for protecting from risk of immaterial and material objects in the context of DiDIY seems to be a good practice.

6. Further work and conclusions

The advent of low-cost digital fabrication technologies and their even lower thresholds to access through collective initiatives such as hackerspaces, FabLabs and makerspaces in general is fuelling the phenomenon of DiDIY. This blurs the lines of professionals and amateurs and offers tremendous opportunities in terms of learning, research, new ways of work and organisation, forms of co-creation and generally increased social affordances. At the same time, it poses threats to many existing legal frameworks.

It is becoming clear that although the current legal systems are evolving through the evolution of technology and society, the core systems have been designed during the early industrial revolutions in the 18th and 19th centuries, and their existence is today seriously questioned. This is in particular the case for IPR regulations. These were put in place as state granted temporary monopolies to provide an incentive for creators and inventors to advance the state of technology and science. However, the success of the Free Software movement over the last 30 years and its many ramifications into other fields of knowledge show that creativity can thrive even without the need for exclusive protection of ideas, industrial designs and creative works.

Considering radical change in such core legal foundations of our society is unrealistic and possibly undesirable, the current system of exclusive IPR rights – in particular as provided by copyright – is however also providing the legal basis for non-exclusive sharing arrangements. Copyright-based free licenses allow authors to share their work granting users all basic rights ("the four freedoms") to enable them full autonomy in their work, thereby allowing the emergence of thriving innovative ecosystems. Having started in the domain of software, this is taking place also in the field of hardware designs. Threats to these open and freedom-respecting ecosystems can come from many sides, with patents being arguably the most complex one to tackle.

In the case of exclusively protected works we have seen how existing exceptions can allow private, non-commercial usage, a feature particularly relevant for the practice of DiDIY. Existing exceptions for interoperability and spare parts reproduction for non-commercial use should be further studied. Such exceptions are particularly relevant in the context of the quest for sustainability and the circular economy, to allow users of commodity products to extend their life through self-made spare parts or custom extensions.

Drone regulations are emerging, while in Europe the non-professional DiDIY practise these are simply referred to as toys and fall under the related regulation. This might prove far too generic and more detailed adjustments can be expected.

The case of liability is another complex area. In simple terms, when products are sold, the so called strict liability doctrine applies, which holds the seller or manufacturer responsible for liability claims. When no commercial transaction can be attributed, there remains a general duty of care. Practitioners of DiDIY can be held liable in cases of negligence. Here lies a challenge of returning to individual responsibilities that society has forgotten about in the age of mass consumerism: when products, their designs, production methods or materials are known to have risks, participants should warn and share appropriately.

Blockchain technology – as known from cryptocurrency Bitcoin – is enabling new decentralised architectures for the collective management of increasingly complex systems. Smart Contracts on the blockchain are executed automatically as computer algorithms and their application in many fields can eliminate the middlemen such as centralised platforms in the collaborative or sharing economy and the Internet of Things. This technology offers great opportunities for innovative democratic self-governance of economic activity of many types, while at the same time it poses

challenges to many regulations. It can be seen as yet another challenge towards systems of central control.

In future work more country-specific details could be studied, which is particularly challenging in such a dynamic field, with national, EU and international legislations evolving in parallel.

Bibliography

Ackermann, J.R. (2009). Toward Open Source Hardware. University of Dayton Law Review. Vol. 34. Nr. 2.

Asay, C. D. (2016). Intellectual Property Law Hybridization, 87 U. Colo. L. Rev. 65.

Ayass, M., Serrano, J. (2012). The CERN Open Hardware License. In: International Free and Open Source Software Law Review Vol. 4, N01: http://www.ifosslr.org/ifosslr/article/view/65.

Bauwens, M. (2005) The Political Economy of Peer Production. Published in CTheory: http://www.ctheory.net/articles.aspx?id=499.

Benkler, Y. (2002). Coase's Penguin, or Linux and the Nature of the Firm. 112 Yale Law Journal 369: http://www.benkler.org/CoasesPenguin.html.

Berkowitz, N.D. (2015). Strict Liability for Individuals? The Impact of 3-D Printing on Products Liability Law, 92 Wash. U. L. Rev. 1019.

Bonaccorsi, A., Rossi, C. (2003). Comparing motivations of individual programmers and firms to take part in the Open Source movement. From community to business: http://flosshub.org/sites/flosshub.org/files/bnaccorsirossimotivationlong.pdf.

Boyle, J. (2008). The Public Domain: Enclosing the Commons of the Mind. Yale University Press: http://www.thepublicdomain.org.

Bradshaw, S., Bowyer, A., Haufe, P. (2010). The Intellectual Property Implications of low-cost 3D Printing. 7 SCRIPTed 5, 26-27: http://www2.law.ed.ac.uk/ahrc/script-ed/vol7-1/bradshaw.asp.

Bradshaw, S. (2013). 3D Printing Legal Update. SCL, The IT Law Community: http://www.scl.org/site.aspx?i=ed32362.

Buterin, V. (2015). Visions Part I: The value of blockchain technology. Blog post: https://blog.ethereum.org/2015/04/13/visions-part-1-the-value-of-blockchain-technology.

Daly, A. (forthcoming). Printing Freedom: Socio-Legal Aspects of the 3D Printing Revolution, Palgrave Macmillan UK.

Daly, A. (2016). Regulating a Revolution: An Introduction to 3D Printing and Law: https://www.academia.edu/25536500/Regulating_Revolution_An_Introduction_to_3D_Printing_and_Law?auto=view&campaign=weekly_digest.

Davidson, S., De Filippi, P., Potts, J. (2016). Disrupting Governance: The New Institutional Economics of Distributed Ledger Technology: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2811995.

DeClercq (2015). The Legal Aspects of 3D Printing from a European perspective, Leiden.

Dolinsky, K. (2014). Untangling Copyrightability, Derivative Works, and Fair Use in 3D Printing, 71 Wash & Lee L. Rev. 591, 595.

De Filippi, P. (2014). Bitcoin: A Regulatory Nightmare to a Libertarian Dream. Internet Policy Review: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2468695.

De Filippi, P., Troxler, P. (2015). From Material Scarcity to Artificial Abundance: The Case of FabLabs and 3D Printing Technologies: http://ssrn.com/abstract=2725404.

DRAFT REPORT with recommendations to the Commission on Civil Law Rules on Robotics. (*2015/2103*(*INL*)).

EASA (2015). Introduction of a regulatory framework for the operation of unmanned aircraft.

Erler, A. (2016). DiDIY and product liability: http://www.didiy.eu/blogs/didiy-and-product-liability.

Falletti, E., Tebbens, W. (2016). Digital Do-It-Yourself Fabrication Practices And Legal Challenges. 12Th IDP Conference (Barcelona 2016): INTERNET, LAW AND POLITICS: BUILDING A EUROPEAN DIGITAL SPACE: http://symposium.uoc.edu/event_detail/3483/sections/4643/llibre-dand39;actes.html.

Federal Trade Commission (FTC) (2015). Internet of Things: privacy and security in a connected world: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

Freeman Engstrom, N. (2013). 3-D Printing and Product Liability: Identifying the Obstacles, 162 U. PA. L. REV. ONLINE 35, 36.

Galli, C., Contini, A. (2015). Stampanti 3D e proprietà intellettuale: opportunità e problemi di una possibile rivoluzione tecnologia, Stampa 3D: una rivoluzione che cambierà il mondo? (C. Galli, C. Zama, eds.), Filodiritto edizioni, Bologna, 2015.

Greenbaum, E. (2013). Three-Dimensional Printing and Open Source Hardware, 2 N.Y.U. Journal of Intellectual Property & Entertainment Law. Vol. 2, Spring 2013, Nr. 2.

Harris, A. (2015). Acting as the consumer and manufacturer, the user must accept the responsibilities of both parties, Journal of Science Policy & Governance.

Iaselli, M. (2015). L'avvento dei droni tra opportunità e problematiche Privacy, Il quotidiano giuridico.

Iaselli, M. (2015). Internet of Things, droni e robotica. Problemi giuridici e possibili soluzioni, Altalex Editore.

Iaselli, M. (2016). Droni cambiano le regole, Altalex, 27 January 2016.

Katz, A. (2012). Towards a Functional License for Open Hardware. International Free and Open Source Software Law Review, Vol. 4 nº. 1: http://www.ifosslr.org/ifosslr/article/view/69.

Lee, E. (2010). Technological Fair Use, 83 S. Cal. L. Rev. 797.

Malone, S. (1970). Ruminations on the Role of Fault in the History of the Common Law of Torts, 31 La.L.Rev.: http://digitalcommons.law.lsu.edu/cgi/viewcontent.cgi?article=3718&context=lalrev.

Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J., Aharon, D. (2015). The Internet of Things: Mapping the Value Beyond the Hype. McKinsey Global Institute, June 2015: http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world.

Margoni, T. (2013). Not for Designers: On the Inadequacies of EU Design Law and How to Fix It. Journal of Intellectual Property, Information Technology and E-Commerce Law.

Mcmeley, C.S. (2014). Protecting Consumer Privacy and Information in the Age of The Internet Of Things, 29 Antitrust ABA 71.

Mendis, D., Secchi, D. (2015). A Legal and Empirical Study of 3D Printing Online Platforms and Analysis of User Behaviour. UK IP Office: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/421221/A_Legal_and_Empirical_Study_of_3D_Printing_Online_Platforms_and_an_Analysis_of_User_Behaviour_-_Study_I.pdf.

Michaelides-Mateou, S. (2015). "Ignorantia Juris Non Excusat": Remotely Piloted Aircraft - Safety Concerns, Violations, and the Need for Awareness, 80 J. Air L. & Com. 423.

Moffat, V.R. (2014). The Copyright/Patent Boundary, 48 U. Rich. L. Rev. 611.

Nielson, H. (2015). Manufacturing Consumer Protection for 3-D Printed Products, 57 Ariz. L. Rev. 610.

Noto La Diega, G., Walden, I. (2016). Contracting for the 'Internet of Things': Looking into the Nest: http://ssrn.com/abstract=2725913.

Opinion WP29 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones, The Swedish Transport Agency´s regulations on unmanned aircraft systems (UAS) (2009).

O'Rourke, M.A. (2000). Toward a Doctrine of Fair Use in Patent Law, 100 Colum. L. Rev. 1177.

Osborn L.S. (2014). Regulating Three-Dimensional Printing: The Converging Worlds of Bits and Atoms, 51 SAN DIEGO L. REV. 553, 571.

Peppet, S.R. (2014). Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent, 93 Tex. L. Rev. 85.

Perritt, H.H., Sprague, E.O. (2015). Drones, 17 Vand. J. Ent. & Tech. L. 673.

Perritt, H.H., Plawinski, A.J. (2016). Making civilian drones safe: performance standards, self-certification, and post-sale data collection, 14 Nw. J. Tech. & Intell. Prop. 1.

Reid, F., Harrigan, M. (2011). An analysis of anonymity in the bitcoin system. In Privacy, security, risk and trust (passat), 2011 IEEE Third International Conference on Social Computing (socialcom) (pp. 1318-1326). IEEE.

Rifkin, J. (2015). The Zero Marginal Cost Society. The Internet of Things, the Collaborative Commons & the Eclipse of Capitalism. Palgrave MacMillan.

Rose, K., Eldridge, S., Chapin, L. (2015). The Internet of Things: An Overview. Understanding the Issues and Challenges of a More Connected World: http://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151022.pdf.

Rosen, L. (2004). Open Source Licensing. Prentice Hall.

Sherwin, E. (2011). Interpreting Tort Law, 39 Fla. St. U.L. Rev. 227.

Strandburg, K.J. (2011). Patent Fair Use 2.0, 1 U.C. Irvine L. Rev. 265.

Szabo, N. (1997). Formalizing and Securing Relationships on Public Networks. First published in FirstMonday: http://www.firstmonday.dk/ojs/index.php/fm/article/view/548. Update: http://szabo.best.vwh.net/formalize.html.

Tebbens, W., Fioretti, M. (2015). The Threats of Dangerous Information. Blogpost: http://www.didiy.eu/blogs/threats-dangerous-information.

Tran, J.L. (2016). Press Clause and 3D Printing, 14 Nw. J. Tech. & Intell. Prop. 75, 79; Volokh E., supra, at 462.

Tushnet, M. (2014). Reflections On The First Amendment And The Information Economy, 127 Harv. L. Rev. 2233,

Volokh, E. (2012). Freedom for the Press As an Industry, or for the Press As A Technology? From the Framing to Today, 160 U. PA. L. REV. 459.

Walport, M. [Chief Scientific advisor to UK Government] (2016). Distributed ledger technology: beyond blockchain. Government Office for Science: London.

Wang, S. (2016). When Classical Doctrines Of Products Liability Encounter 3D Printing: New Challenges In The New Landscape, 16 Hous. Bus. & Tax L.J. 104.

Weinberg, M. (2010). It Will Be Awesome if They Don't Screw It Up: 3D Printing, Intellectual Property, and the Fight over the Next Great Disruptive Technology, Public Knowledge: http://www.publicknowledge.org/files/docs/3DPrintingPaperPublicKnowledge.pdf.

Williston, S. (1959). A Treatise of the Law of Contracts. Third Edition by Walter H.E. Jaeger. Vols 1 and 2. Mount Kisco New York. Baker, Voorhis and co.