# jipitec

4 | 2013

Volume 4 (2013)
Issue 1
ISSN 2190-3387

## Articles



## Reports



## Book Reviews





Journal of Intellectual Property, Information Technology, and Electronic Commerce Law

www.jipitec.eu

jipitec

Journal of Intellectual Property, Information Technology and Electronic Commerce Law

Volume 4 Issue 1, 2013
www.jipitec.eu
contact@jipitec.eu

A joint publication of:

Prof. Dr. Thomas Dreier, M. C. J.,
Karlsruhe Institute of Technology,
Vincenz-Prießnitz-Str. 3,
76131 Karlsruhe

Prof. Dr. Axel Metzger, LL. M.,
Institute for Legal Informatics,
Leibniz Universität Hannover,
Königsworther Platz 1,
30167 Hannover

Prof. Dr. Gerald Spindler,
Dipl.-Ökonom, Georg-August-Universität Göttingen,
Platz der Göttinger Sieben 6,
37073 Göttingen

Karlsruhe Institute of Technology, Leibniz Universität Hannover, and Georg-August-Universität Göttingen are corporations under public law, and represented by their respective presidents.



ISSN 2190-3387

Funded by
DFG Deutsche Forschungsgemeinschaft

# Table Of Contents

## Articles



## Reports



## Book Reviews

# "Privacy by Design": Nice-to-have or a Necessary Principle of Data Protection Law?

by **David Krebs***
Juris Doctor, LL.M., Member of the Law Society of Alberta (Canada)

**Abstract:** Privacy by Design is a term that was coined in 1997 by the Canadian privacy expert and Commissioner for Ontario, Dr Ann Cavoukin, but one that has recently been receiving more attention in terms of its inclusion as a positive requirement into EU, US and Canadian data protection frameworks. This paper argues that the right to personal privacy is a fundamental right that deserves utmost protection by society and law. Taking privacy into consideration at the design stage of a system may today be an implicit requirement of Canadian federal and EU legislation, but any such mention is not sufficiently concrete to protect privacy rights with respect to contemporary technology. Effective privacy legislation ought to include an explicit privacy-by-design requirement, including mandating specific technological requirements for those technologies that have the most privacy-intrusive potential. This paper discusses three such applications and how privacy considerations were applied at the design stages. The recent proposal to amend the EU data protection framework includes an explicit privacy-by-design requirement and presents a viable benchmark that Canadian lawmakers would be well-advised to take into consideration.

**Keywords:** Data Protection, Canadian Privacy Law, Comparative Law, EU Data Protection Regulation, Right to Privacy



Recommended citation: David Krebs, "Privacy by Design": Nice-to-have or a Necessary Principle of Data Protection Law?, 4 (2013) JIPITEC 2, para. 1.

## A. Introduction

1 The threats to the individual right to privacy – or what is sometimes referred to as the right to 'informational self-determination'[1] or simply the 'right to be let alone'[2] – are currently being widely discussed, debated and analysed. This is particularly so where this right is impacted by new technologies or the incremental move of our daily activities online. New technologies that impact the way in which information about people, 'personally identifiable information'[3] ('PII'), is used, collected, stored and disseminated are appearing at a frequent and rapid pace. These may be 'apps', facial recognition technologies, smart electricity grids, Radio Frequency Technologies (RFID), cloud computing, mass and surreptitious surveillance, biometrics and private sector Internet marketing initiatives. Currently, for the most part at least, technology is being adjusted after the fact to patch privacy-related issues as they arise or after they have already had a negative impact.

2 To address these concerns and to move from a reactive to a proactive approach, Dr Ann Cavoukian, current Privacy Commissioner for Ontario, in 1997 had already developed the principles behind – and coined the phrase – 'privacy by design' (PbD). PbD recognizes that the deployment of technologies designed to achieve a certain commercial or public sector goal *without* having considered the privacy implications at the design stage of the technology[4] can result in personally identifiable information (PII) being used or disclosed in ways that harm privacy rights permanently. PbD embodies the merger of

two objectives: the protection and control of PII and privacy, and the advancement of the commercial application of technologies in a sustainable but competitive manner.[5] The *Protection of Information and Electronics Documents Act*[6] ('*PIPEDA*')[7] (as well as the *European Data Protection Directive*)[8] contains provisions relating to the adequacy of protective security measures and also, implicitly, privacy 'by design' requirements. At present, however, PbD is not an explicit part of the legislative scheme in Canada, the European Union (EU) or the United States of America (US), even though it is often cited as a best practice and perhaps even as the 'gold standard' in privacy protection.[9]

3 Calls for an introduction of PbD into legislative frameworks have been receiving more attention recently, for example, within the proposal for an EU privacy framework,[10] in proposed legislation in the US,[11] as well as a resolution at the *32nd International Conference of Data Protection and Privacy Commissioners* in Jerusalem. In Canada, there have been no such concrete proposals, only the vocal views of the Federal and Ontario Commissioners.

4 This paper argues that legislated PbD is the necessary next step in privacy law to protect a right that is fundamental to liberty, personal integrity and democracy. For this reason, PbD deserves explicit mention as a tenet of privacy and data protection law. However, the view that laws based on PbD principles alone would be sufficient in this regard is not tenable in a world of ubiquitous computing and transformative technologies. A broad, principled approach relies on organizations adopting appropriate measures without providing the necessary guidance necessary to *prevent* actions injurious to personal privacy such as data breaches, unwanted tracking or uncontrolled collection of ever-increasing amounts of PII. PbD needs to be incorporated into the privacy law framework in Canada (and elsewhere) as a general organizational requirement *and*, in appropriate circumstances, mandate specific technological solutions, such as 'privacy enhancing technologies'[12] (PETs), as well as the corresponding ability for the regulator to prevent a system or application from being initiated.

5 The first part of this paper will briefly describe the legal right to privacy in order to set the stage for why the design of systems that conform to this right is of such primal importance to its ultimate protection. The second part will turn to the current legislative framework to canvass the extent to which current provisions would satisfy the needs intended to be addressed by PbD. In this section, I will include examples from the EU framework because of its relevance to Canadian privacy laws. Canadian policy discussions often run in parallel[13] and Canada and Europe share many relevant socio-cultural aspects.[14] I will also be looking to the US, where there have been some significant developments in this regard. The third part will look at pertinent examples of systems to which PbD principles were applied, and without which the resulting systems would likely have been much more privacy-intrusive. The last part of the analysis will focus on the views of data protection authorities relating to incorporating PbD into legislative frameworks, including a close look at the legislative proposal from the Ontario Commissioner, Dr Ann Cavoukian, which was included as part of a very recent publication from her office.[15] The final part of this article will make some recommendations and suggested points for future research in this regard.[16]

## B. Privacy by Design

### I. The Right to Privacy

> [Code] will present the greatest threat to both liberal and libertarian ideals, as well as their greatest promise. We can build, or architect, cyberspace to protect values that we believe are fundamental. Or we can build, or architect, or code cyberspace to allow those values to disappear.[17]

6 This section is not intended to provide an exhaustive background to or a detailed comparative analysis of the right to privacy in Canada versus other Western jurisdictions.[18] Rather, it is intended to set the stage for the discussion of why a legislated PbD requirement might be a necessary addition to existing data privacy frameworks in order to protect the right to privacy as a fundamental personal and democratic right.

7 In some jurisdictions, privacy is an explicitly stated constitutional right.[19] In the EU, all Member States are signatories to the *Convention for the Protection of Human Rights and Fundamental Freedoms* (ECHR),[20] which incorporates privacy as a fundamental right into EU law. Article 8 of the ECHR protects the "Right to respect for private and family life'[21] and forms the basis for modern privacy protection in Europe.

8 In Canada, the right to privacy is not a constitutional right as such; rather, the constitutional right to privacy is rooted in and protected by the Supreme Court of Canada's interpretation[22] of Section 8 of the *Charter of Rights and Freedom,*[23] the right to be free from unreasonable search and seizure. This protection is similar to the right afforded by the American 4th Amendment,[24] although one should not go too far in drawing parallels, as the jurisprudence in the US and Canada in this regard is certainly not uniform. Section 8 protects the liberty of the person but only in so far as the individual has a

'reasonable expectation of privacy'[25] in the conduct that is impacted by the intrusion or violation at the hands of the State, not applicable to intrusion by the private sector. Thus, constitutional protection of this privacy right is limited to where there is an infringement by the State of an individual's reasonable expectation of privacy.[26] It is by no means an absolute constitutional right.

**9** Other than the protection of liberty, privacy rights have been stated to encompass two other values, informational privacy and dignity of the individual.[27] The Supreme Court of Canada in *R. v. Dyment*[28] noted that *Charter* privacy rights protect three aspects: spatial, informational and personal. Informational privacy rights in Canada are not constitutional rights. They are protected by private and public sector federal legislation such as *PIPEDA* and the *Privacy Act*,[29] respectively, as well as by relevant provincial and sector-specific legislation.[30] The European notion of privacy as the protection of dignity and democratic values[31] has been stated to exist as the third pillar of privacy protection in Canada and is related to the fact that the Canadian basis for privacy protection lies in the right to informational autonomy rather than solely in the right to liberty of the person.[32] It has thus been called the 'middle ground' or a compromise between the US and EU approaches.[33]

**10** Privacy rights are clearly entrenched in Canadian jurisprudence and constitutional law. They are not rights that have been recently imagined but are deeply entrenched in Canadian and European culture. However, these laws stem from a time before most of the privacy-invasive technologies we are faced with today were a factor or even conceivable. They originated in a time before ubiquitous social media applications, before cloud computing, before Google Street View and before tracking technologies such as radio frequency identification devices (RFID)[34] existed or at least were in use; and although the principles may be sound, they cannot currently cope with systems and applications that were, for the most part, not designed with privacy protection as a main consideration. The key might lie in using the PbD approach to bridge the gap between ever-forward-moving technology and laws that (one could say inherently) lag behind. But before exploring why it might be necessary to include PbD within *PIPEDA* and other privacy legislation as an explicit requirement, the section below will outline the principles of PbD as well as salient examples of where these principles have been applied applications.

## II. General Principles of PbD

**11** PbD is no longer the exclusive domain of the Ontario Commissioner. As we will see throughout this paper, many other privacy experts have contributed to its definition, application and scope. That being said, the core principles enumerated by Dr Cavoukian are called the '7 Foundational Principles'[35] of PbD and still form the basis of what PbD encompasses. These include the following (not in order of importance): 1) proactive not remedialpreventative not reactive; 2) privacy as the default; 3) privacy embedded into design; 4) positive sum not zero sum; 5) end-to-end security; 6) visibility and transparency; and 7) respect for user privacy.

**12** There is no hierarchy among these principles. Together they form the PbD objective in systems design: ensuring privacy, gaining control over one's information, and, for organizations, gaining a 'sustainable competitive advantage'.[36] The German Federal Commissioner for Data Protection and Freedom of Information ('German Commissioner'), Peter Schaar, himself a proclaimed 'PbD Ambassador',[37] recently distilled six PbD principles that should be taken into account in the design or acquisition of a processing system: data minimization, controllability (possibility of consent and objection supported by technological means), transparency, data confidentiality (security), data quality and possibility of segregation (in multi-user environments such as virtual machines and cloud computing).[38]

**13** The German Commissioner has taken on the original foundational principles and to a limited, but I would argue important, extent altered or at least tweaked their meaning. For one, his PbD is prescriptive from a technological perspective. Secondly, the German Commissioner does not put as much emphasis on the 'win-win'[39] of technological advancement and the protection of privacy. PbD must first and foremost ensure that the principles of the EU Directive and the constitutional right to privacy are protected. Commercial interests are by no means a lone afterthought; rather, they seem to stand more on the periphery of the German Commissioner's notion of and purpose of PbD when compared with the description of the 7 Foundational Principles by the Ontario Commissioner.

**14** In the United States, the debate surrounding PbD as a mandatory part of a legislative framework centres around organizational obligations, rather than embedded technological solutions to protect privacy by default, such as PETs.[40] The view that privacy is a right to be free from intrusion rather than a right to informational self-determination is more prevalent in the US than Europe or Canada. Underlying this rationale is the belief that commercial actors should have the freedom to control the means of processing data as long as they adhere to certain sound and proportional organizational principles. In the US, the term 'privacy' has more to do with harm, fear and the threat posed by computers than with the

general European view that to protect privacy is to protect personality and democracy. [41]

**15** With the more pronounced 'positive sum' statement, the IPC – although at first glance aligned with the European approach, in particular when considering principle '3' of the PbD principles – lies somewhere in the middle of the purely organizational-measure and more prescriptive notions of PbD. The IPC states no official preference of whether a mandatory PbD requirement should be more organizational or technological, only that it encourages the adoption of PbD requirements into legislation in *some* form.[42]

**16** Overall, PbD is still a relatively vague concept in terms of its translation into concrete systems design. Part of this is attributable to its relative novelty, at least in its widespread usage, and the other part to the gap that exists between regulators and systems engineers.[43] The 7 Foundational Principles, just as the US Federal Trade Commission's (FTC) and EU Commission's most recent interpretations, have been criticized as representing a 'non-technical' strategy to privacy that lacks technological guidance on PbD application.[44] While there may be many unresolved issues surrounding the practical implementation of PbD in certain instances, there are also numerous examples of feasible and successful applications from which important lessons can be drawn with respect to the utility, importance and implementation of PbD.

## III. Current Practical Applications of PbD

**17** PbD has a vast array of potential applications. In fact, any system that processes PII could benefit from or be the subject of PbD principles. This section will describe three examples of where PbD principles were considered in the design of systems that process large amounts of PII: the Smart Grid roll-out in Ontario, the use of biometrics for identification and the ELENA project in Germany, and the welfare application system in Ontario. I would argue that the application of PbD for all these systems was successful notwithstanding the very different practical outcomes for the introduction of the systems themselves.

### 1. Smart Grid

**18** The term Smart Grid[45] refers to a system in which energy is delivered to the end-consumer in a way that allows for a more stable power supply, time-use pricing and demand management using state-of-the-art telecommunications to enable the 'smart' meter to communicate with the source.[46] The fact that energy supplies are decentralized to a much larger extent than years ago, while consumers have the ability to turn appliances off and on when they choose, creates the potential for energy supply-side instability. This is exacerbated where renewable energy is introduced into the system (as a less predictable supply of energy). This load-balancing could be achieved by creating the so-called 'Smart Grid', an intelligent grid that envisions two-way communication between demand (household) and supply (power source).[47] On account of its *ad hoc* ability to adjust the supply of energy, the Smart Grid can effect energy savings, and therefore also has positive environmental implications. It is estimated that by 2015 there will be 250 million smart meters installed worldwide.[48]

**19** A more technical description of the Smart Grid is that it encompasses three aspects: Virtual Power Plants (VPP), Demand Side Management (DSM) and Control of Supply.[49] A VPP would be the backbone of the system, connecting a range of distributed and separate power supplies (windmills, solar or another other source of energy) that could then be managed according to demand. The VPP reduces the volatility of each individual power supply, as can be the case especially for renewable energy sources like wind and solar. The second part of the system is DSM, which is aimed at controlling demand. This control can either be initiated by the consumer (by reducing consumption) or by the supplier directly, whereby the consumer would agree to permit the operator to actively turn on and off certain appliances to balance energy use. The third piece of the puzzle is the control of the actual flow of power from the source to the end-user.

**20** This intelligent system relies on information provided to the supplier by the household. This information is at least *prima facie* PII as it is naturally linked to a home, which in many cases will be owned and occupied by an individual. The type of information typically collected by the system (by way of 'Smart Meters'[50] installed at the home) will relate to the household's energy consumption patterns. Depending on the particular system and the incorporation of direct DSM or even 'Smart Appliances'[51], the information collected, however, will reveal a great deal more about the individuals than pure energy consumption. It may indirectly reveal criminal activities in the home, family living patterns, status of health, indications of physical activity in the home (types of machines) and so on. The use of the information is therefore not only relevant to the efficient control and supply of energy (utility services) but also for so-called 'edge services'[52] and law enforcement, insurance and market research purposes.[53]

**21** Quite obviously, this system by its nature, and in particular if not designed properly, has immense negative implications for privacy and the protection

of the data entrusted into the system. Apart from the potential misuse of more traditional energy use data that is communicated via the system, the Smart Grid itself creates *new data*, not in existence before (e.g. relating to smart appliances), which is then also vulnerable and perhaps even more attractive for secondary uses. Beyond this, the National Institute of Standards and Technology (NIST) found in a Privacy Impact Assessment (PIA) conducted on Smart Grid systems that one of the major privacy risks of Smart Grids is the lack of consistent and comprehensive privacy policies among all the players whose actions affect PII (government agencies, utility companies and supporting organizations).[54]

**22** For the Ontario Smart Grid implementation, the IPC and energy providers worked closely together to operationalize the system to include PbD aspects, that is, to design the way in which the system would operate and process PII throughout its life cycle. This project had and has implications for the design of Smart Grids elsewhere in Canada and internationally. The NIST has recently recommended the PbD approach as an appropriate methodology in this respect.[55]

**23** This project focused on a number of issues that would need to be addressed operationally as well as technologically within the system and was described in great detail in a joint paper written by the system's operator, Hydro One, its partners and the Ontario Commissioner.[56] In this particular case (this method could also be applied to other systems), incorporating PbD meant that its principles needed to be part of the so-called Architectural Decisions document. This document defined the base policies and procedures that needed to be adhered to throughout the entire project and throughout all three 'domains' of the grid (the home domain, including smart appliances and meters; the services domain, including host data; and the grid domain, with the software backbone that automates and controls the distribution grid).

**24** Including PbD into the entire system meant that

a) for the customer/home domain, no PII would persist on any device from the services to the customer domain (unless other services are explicitly purchased and consented to by the user); no PII will be sent from the services domain to the customer domain; and any interfacing online will include appropriate identity management and protection of information tools;

b) for the services domain, any and all access to devices in the customer domain from the services domain will be restricted and recorded; direct access must be authorized by the end-user; strict authorization-based access controls must be implemented whenever there is access to the customer domain; and all management of data storage would follow industry practices; and

c) for the grid domain, no PII will persist on any device in the grid domain; information regarding a device will be provided using authorized services; and access to a device must also be conducted through authorized services within the serviced domain.

**25** Today, the Smart Grid is still in its relative infancy. Even in Ontario, a world leader in this regard (all residential homes have been equipped with smart meters), [57] the grid is not operational to its full capability.[58] Implementing PbD will thus be an on-going endeavour as the Smart Grid gets 'smarter' and more pervasive.[59] The design of these systems will require continuous evaluation in proportion to the granularity and amount of consumption data that is processed,[60] and the perils of the Smart Grid in terms of privacy impact are known and discussed on an on-going basis.[61] As it stands, however, the design of the Smart Grid in Ontario is by and large a positive example of how privacy considerations are being designed into a complex system from the outset. That is the strength of PbD: it is architected into the DNA of a system, and this is something that may not be fully guaranteed by laws that focus on principles rather than prescriptive standards.

## 2. ELENA

**26** A second example of a system to which PbD principles have been applied is the 'ELENA' system in Germany. It stands for '*elektronischer Entgeltnachweis*' (electronic proof of earnings) and refers to a database system in Germany designed to store income information for all individuals employed in Germany for the purpose of streamlining applications for certain social benefits. ELENA as a process and system was designed as follows: Prior to applying for a certain benefit, an applicant would first obtain an electronic signature card with a smart chip containing a 'qualified electronic signature'[62] from a (government-certified) certification service provider. This step provides proof of an individual's identity. This unique signature card is then registered with the appropriate authority. The 'registry process' then links the certificate ID with the social security number of the applicant. On the ELENA database, then, employee personal data is not linked to the social security number of the applicant, but to the ID number of the certificate for the registered chip card. The card itself contains no information other than the name of the applicant and ID number of the registered chip card. All other information is stored in the central ELENA database.[63]

**27** Due to the amount and sensitivity of PII, this database received considerable public attention. As noted previously, German privacy rights are explicitly entrenched in its Basic Law (*Grundgesetz*), and so this may have contributed to the German Commissioner being involved at a very early stage of the development process. The principles of German data protection law that were explicitly incorporated into ELENA included the following: encryption of all communication channels and data; separation between the central database and responsible administering body; logging of all database transactions; rigorous deletion of expired or unnecessary data; the principle of requiring the (qualified electronic) signatures of both data subject and administering body; and no access to security, tax or customs authorities.[64]

**28** Ultimately, the application of PbD principles contributed to the current abandonment of the plans to bring the system online. Originally it was planned for ELENA to become operational as of 1 January 2012. Then, in July 2011, it was announced that the implementation of ELENA was to be abandoned[65] and that all PII collected to date was to be destroyed or deleted. The stated reason was that qualified electronic signature cards had not found widespread application. As a cornerstone of ELENA's functioning (and coinciding data protection and security standards), the widespread use and accessibility of the qualified electronic signature[66] was seen as an indispensable condition precedent to the system's implementation. According to most estimates, ELENA has cost Germany's taxpayers hundreds of millions of euros.[67]

**29** The Smart Grid and ELENA systems are both examples of how PbD is and was applied and what the outcomes might be if the principles are applied appropriately. As we have seen, PbD can result in a system becoming a functioning data protective system, or it may result in the system being abandoned because its design cannot be reconciled with privacy principles.

### 3. Ontario Social Works Act

**30** The third and final example of successful PbD application[68] is the welfare application system in Ontario. To combat abuse[69] of the social welfare system, in 1997 the Ontario government proposed certain changes[70] to the *Ontario Public Works Act, 1997*[71] and the *Ontario Disability Support Program Act, 1997*[72] enabling the ability to require welfare applicants to submit biometric data – here fingerprints – as unequivocal proof of identity when applying for benefits.[73] The privacy implications were grave since it would involve the collection and storage of sensitive, uniquely identifying data which would then be used in an assessment which is in and of itself of grave import to the individual applicant as it involves basic financial assistance.

**31** With a view of balancing this processing of sensitive data with the need to combat fraud in the welfare system, the Ontario government worked with the IPC very early on in the process. After this consultation, it was decided that biometric data could be collected and used, but only if the concrete requirements relating to privacy and security of the information were followed. These are now entrenched in Section 75 of both pieces of legislation, and include requirements that any biometric information must be encrypted and destroyed after the encryption process, collected directly from the individual, only be released to third parties on warrant, and only retain address and sex alongside the encrypted biometric information.

**32** Some of the above requirements now included in the legislation relate to processes, some to security measures and others to actual technology, but it is clear that not involving these measures at the outset[74] would have left this sensitive data exposed significantly more because a system architecture, once in place, is very difficult to re-design.[75] A system could be compliant with *PIPEDA* (or in this case, provincial public sector legislation) without fulfilling all of the principles of PbD, in particular when it comes to the requirement that all data would need to be encrypted and then destroyed after the process was complete, which is not an explicit requirement[76] under *PIPEDA*, leaving the data within the system more vulnerable to misuse and unauthorized access. It is important to note that the use of these systems was tabled in the public realm and therefore scrutinized before inception. For governments, this political pressure is a natural incentive to go beyond the letter of the law to protect citizens' privacy rights, but private companies that can implement systems out of the public's sight will not be subject to the same level of scrutiny, and one would expect deliberations to be based primarily on feasibility, cost and compliance with the law rather than the protection of privacy as such.

## IV. Current Relevant Legislative Landscape

### 1. Canada

**33** Canada's public and private sectors are governed by separate pieces of legislation both at a federal and provincial level. *PIPEDA* is federal legislation and governs private sector organizations, while the *Privacy Act* governs the public sphere. The Provinces each have separate public sector legislation, but only four (Alberta, Saskatchewan, Manitoba and

Ontario) have specific[77] health-sector legislation. Essentially, *PIPEDA* applies to the processing of personal information relating to all commercial activities where there is no provincial private-sector legislation, as well as to inter-provincial and international personal data flows, but it does not regulate activities related to the personal information of employees of provincially regulated organizations.

**34** At a provincial private-sector level, only Alberta, Quebec and British Columbia have enacted their own pieces of commercial private-sector legislation, and within those Provinces, *PIPEDA* only applies to federally regulated organizations, including the personal information of employees of those federal organizations.

**35** As a result, Canada does not have a uniform privacy framework. Compared with the EU (where Member States themselves – such as Germany, for example – may have a federal-provincial system comparable to that of Canada), however, these differences are still quite minor and one can speak of a relatively cohesive legislative landscape.[78]

**36** Neither *PIPEDA* nor any of the provincial equivalents contains an explicit PbD requirement. What the legislation does require is adherence to the privacy principles of the *CSA Model Code for the Protection of Personal Information*,[79] which by *implication* may require data privacy considerations at the design stage of a system. A salient example of this would be Principle 4.7 regarding 'safeguards' (some of the suggested technological measures would need to be contemplated before bringing a system online) as well as Principle 4.4 regarding 'limiting collection'. This implicit application of PbD has become apparent during investigations of the Office of the Privacy Commissioner of Canada (OPC), for example, the *Google StreetView* Case,[80] in which Google was investigated for collecting PII in contravention of *PIPEDA*. Several of the remedial measures related to design-stage considerations (e.g. technical documents and evidence of appropriate processes and training ensuring that these are implemented when new systems are rolled out). The Commissioner applied Principle 4.4.1, which prohibits 'indiscriminate' collection of PII. As the collection of data is at the front end of any data processing, it is hard to imagine that this principle could be adhered to without giving thought to privacy considerations at the design stage.

**37** All that being said, the requirements on Google to implement specific features *specifically* at the design stage would likely have been more explicit, and thus the protection of PII stronger, if a separate principle could have been relied on. As an example of this, on a number of occasions it was noted that privacy had not been considered sufficiently during the design of certain products, but the Commissioner did not have the ability to specifically state that a *PIPEDA* principle was breached. PbD remained an element of the ultimate recommendations, but only on the periphery.

**38** A relevant feature of *PIPEDA* is the principle of "Accountability",[81] which requires organizations to designate individuals to "oversee the organization's compliance" with the principles contained in *PIPEDA*. Organizations need not notify the OPC of their PII processing activities (as in the EU, to be discussed below) but remain directly accountable for non-compliance under this principle. The OPC has the ability to audit such compliance. A weakness of *PIPEDA* from an enforcement perspective is that the Commissioner must initiate a complaint via the Federal Court, and only the Court may *force* an organization to correct its practices.[82] That is, *PIPEDA* currently does not contemplate the prevention of a system from being implemented, and this to be enforceable by the OPC, other than by the organization's accountable person to ensure that the Act is being complied with. Having a PbD requirement would obviously assist this individual in making an argument that certain requirements *must* be adhered to prior to going live with the processing.

**39** Bill C-12, *An Act to Amend the Personal Information Protection and Electronic Documents Act*,[83] is currently in the first reading in the House of Commons and does not contain any mention of PbD as part of its amendments, which, apart from breach notification requirements, do not enhance the protection of PII in Canada but rather the ease of processing PII. As the analysis below will illustrate, this absence bucks the trend in other jurisdictions as well as to a certain extent the views of privacy commissioners and experts in this regard and may even be unsustainable[84] *vis-à-vis* a new EU data protection framework.

## 2. European Union

**40** The basic data protection framework consists of the Data Protection Directive, the Directive on Privacy and Electronic Communications (e-privacy Directive),[85] the Data Retention Directive[86] and the 2009 e-privacy Directive.[87] All EU Member States have implemented the 1996 EU Directive. One must remember, however, that data protection law is by no means harmonized across the EU and that all statements about the 'European' situation must be viewed from this perspective. That is, the Directive is a guiding instrument (not a 'Regulation' with direct effect on local national law) and its intention is to harmonize the protection of PII within the otherwise free flow of information between Member States; in reality, however, there are many different laws and regulations (and underlying cultural aspects)

relating to the protection of personal data within the EU borders. Essentially, the EU has 27 similar but separate data protection laws. Sweden, as an example, views data protection law not as an equal guarantor for privacy and the free flow of information but primarily as a mechanism to ensure that a person's 'integrity' is not harmed by the use of PII (Section 1 *Personuppgiftslagen*[88]),[89] whereas this notion is not mentioned in the UK *Data Protection Act*.[90] Germany's federal law includes data breach notification provisions, which are not mandated by the EU Directive and provide a good example of the EU Directive provisions being a baseline of protections which local law may enhance under applicable circumstances.

**41** The German Commissioner has pointed out on a number of occasions[91] that PbD is to a certain extent already regulated by the Directive by way of Article 46 of the recitals,[92] wherein it states:

> Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires *that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself,* particularly in order to maintain security and thereby to prevent any unauthorized processing; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, *taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected* (emphasis added).

**42** I would argue that this is also implicit in Article 2 of the recitals:

> Whereas *data-processing systems are designed to serve man*; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals (emphasis added).

**43** The Article 29 Working Party has opined that PbD should in fact become part of the revised Data Protection framework in Europe.[93] A closely related principle which also deserves explicit incorporation is the principle of 'accountability'. As noted, *PIPEDA* includes this principle as part of the *CSA Model Code*. This principle requires every organization to appoint one person within the organization to be accountable for the management of the organization's PII. The link to the PbD principle is that organizations would be required to ensure that this principle is being adhered to, as well as demonstrate compliance when challenged. The EU Directive also contains a notification requirement (Article 20). This obliges organizations to notify the appropriate DPA of PII processing in advance. In practice this means that a DPA may be able to prevent a system from going live, and this element of the Directive provides a complement to any PbD requirement as both are pre-emptive in their aims.

**44** The European DPA wishes to not only see PbD included into the EU framework as a general principle but as a requirement for specific applications, specifically RFIDs, social networking applications, and browser applications. These requirements would be binding not only on data controllers[94] but also on processors, designers and purchasers of systems or applications.[95]

**45** This approach is quite prescriptive and more what the Ontario Commissioner has called 'command and control regulation'.[96] It is clear from the EU DPA's perspective that loose principles will not suffice when systems with a potentially profound impact on privacy rights are concerned.

**46** The very recently released first draft of the proposal of the European Commission to revise the EU Directive marks a big step toward the likely adoption of PbD into European (and other pieces) legislation. It is an ambitious attempt at harmonizing the EU legislative landscape. The proposed framework is suggested as a 'Regulation'[97] (with direct effect on Member States rather than a "directive which must then be transposed into local laws). This is in and of itself a major step toward harmonization. The Proposal includes a host of significant amendments, including doing away with the requirement to notify of processing[98] and replacing it with the obligation to maintain appropriate documentation surrounding the processing on controllers and processors (Article 28), explicit consent requirements (Article 1 – 'informed and explicit'), as well as a 'right to be forgotten' (Article 17) and a data breach notification requirement (Article 32). Most importantly for current purposes, the proposal includes a PbD requirement (Article 23) as follows:

1. Having regard to the size of the organization and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

2. The controller shall implement mechanisms for ensuring that, by default, only those personal

> data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.
>
> 3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 *for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms* referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.
>
> 4. The Commission *may lay down technical standards* for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

**47** Although it takes into account the state of the art and cost of implementation, it obliges the controller of PII to implement technical and general organizational measures at the design stages of PII processing, as well as privacy by 'default' settings, itself an integral component of PbD. Beyond these generalist principles it contemplates specific technical standards to be set by the Commission. While we do not know how this will be implemented in practice, it is certain that the Proposal goes beyond the self-regulation and principle-only approaches described previously herein. The Proposal also places the obligation to monitor application and implementation on a 'Data Protection Officer' (DPO). The obligation to appoint a DPO to represent public organizations and 'large enterprises or where the core activities of the controller or processor consist of processing operations which require regular and systematic monitoring is also among the proposed changes'.[99] This requirement is not new[100] for all Member States and builds on the current Directive which contemplates the possibility of DPO appointment. To complement these changes to the framework, the potential penalties associated with breaches were increased: up to two (2) percent of annual global turnover for the gravest breaches. The coming year will shed light on the reactions to the Proposal and will provide valuable guidance on the likely development of PbD and other aspects of international privacy law.

## 3. United States

**48** At a federal level, the US does not currently have omnibus private-sector privacy legislation. The current framework in the US is a patchwork of sector-specific state and federal level legislation. The *Commercial Privacy Bill of Rights Bill of 2011*[101] is an attempt to introduce such legislation and was brought forward by Senators John Kerry and John McCain mid-2011 as an attempt to regulate the private sector's use of PII at the federal level. The Bill has received both praise[102] and criticism,[103] but notwithstanding this early controversy, it is so far the first piece of legislation in North America to include mention of 'privacy by design' as part of a mandatory privacy framework. Although it has recently stalled somewhat, the advent of the new EU Proposal may see a rejuvenated debate surrounding this Bill.

**49** Section 103 specifically mentions the term 'privacy by design':

> Each covered entity shall, in a manner proportional to the size, type, and nature of the covered information that it collects, implement a comprehensive information privacy program by
>
> '(1) incorporating necessary development processes and practices throughout the product life cycle that are *designed to safeguard the personally identifiable information* that is covered information of individuals based on
>
> (A) the reasonable expectations of such individuals regarding privacy; and
>
> (B) the relevant threats that need to be guarded against in meeting those expectations [...]'

**50** Whether the Kerry-McCain idea of privacy by design can be considered to fulfil the principles of PbD envisioned by the Ontario Commissioner is arguable; nevertheless, its mention signals the importance of privacy considerations implemented early on in the systems design process.

**51** Another US example of design-stage privacy considerations is the FTC's decision regarding Google's Buzz social media application. The FTC, under Section 5 of the *Federal Trade Commission Act*,[104] has the power to prohibit unfair and deceptive trade practices. Non-adherence to privacy policies or deceptive privacy policies has been considered deceptive by the FTC under this section, most notably in the Google Buzz case.[105] In the FTC's order, Google was ordered to maintain a comprehensive five-step privacy program (auditable by the FTC for a period of 20 years):

> A. the designation of an employee or employees to coordinate and be responsible for the privacy program.

> B. the identification of reasonably foreseeable, material risks, both internal and external, that could result in the respondent's unauthorized collection, use, or disclosure of covered information, and an assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this privacy risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management, including training on the requirements of this order, and (2) *product design*, development, and research.
>
> C. *the design and implementation of reasonable privacy controls* and procedures to address the risks identified through the privacy risk assessment, and regular testing or monitoring of the effectiveness of those privacy controls and procedures.
>
> D. the development and use of reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from respondent, and requiring service providers by contract to implement and maintain appropriate privacy protections.
>
> E. the evaluation and adjustment of respondent's privacy program in light of the results of the testing and monitoring required by subpart C, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its privacy program.

**52** This 'privacy program' is also somewhat of an implementation plan for PbD in that it refers to the actual design stages of systems. In a recent publication by the FTC,[106] PbD was specifically enumerated as a cornerstone of the future of privacy protection:

> First, companies should adopt a 'privacy by design' approach by building privacy protections into their everyday business practices. Such protections include providing reasonable security for consumer data, collecting only the data needed for a specific business purpose, retaining data only as long as necessary to fulfill that purpose, safely disposing of data no longer being used, and implementing reasonable procedures to promote data accuracy.

**53** The US approach focuses on organizational measures while providing individual organizations a relative large amount of leeway regarding the translation of these design requirements. While this may call itself 'privacy by design', it may not actually be a huge step beyond those laws which already exist in the EU and Canada, at least when they are interpreted broadly. Privacy by design in the US does not mean the same thing as that very same term does in the EU or Canada, as evidenced by the Kerry-McCain Bill and the language used by the FTC. What the US approach does accomplish, however, is that it specifically mentions PbD and provides a solid basis for increased personal data protection at the design stage of personal data processing systems and associated products.

## C. Current Views on Mandatory PbD

**54** The debate surrounding a legislated PbD requirement can be characterized by three main perspectives: 1) having PbD features embedded into systems, including mandating certain technological features such as privacy by default and PETs within those systems (advocated, *inter alia*, by the Article 29 Working Party); 2) making PbD a legislative organizational requirement to the extent that it should be adopted as a general principle of data protection law, without requiring specific regulation of specific technologies (more or less the 'US approach' described in the previous section); 3) PbD is not to become part of a legislative framework but rather as part of a self-regulatory initiative and encouraged as an industry best-practice. Some of those who hold the latter view also consider PbD redundant as it is already contained in the current legislative framework in the EU (and so therefore also Canada) and no additional burdens should be placed on industry.

**55** The view that PbD should not be part of a legislative scheme is based on three main arguments: it would stifle innovation and place a disproportionate burden on economic operations,[107] it is unnecessary because it is already contained in the current framework (under Articles 6 and 17 of the EU Directive), and a legislated PbD requirement would not achieve the desired outcomes of protecting privacy but would in fact stifle the innovation necessary to drive privacy protective technologies and practices forward:

> Similarly, privacy-by-design is not something that, in itself, can be mandated by regulation. But intelligently crafted regulatory incentives can be built to encourage this movement. Instead, in today's world of global data flows, organisations need to see the value of appointing an officer in charge of privacy programmes and compliance, or in an approach to privacy risk management that seeks to engineer solutions through better product design, rather than the legalistic 'bolt-on' approach favoured today by most lawyers. The Commission must think through the most effective options for incentivising

these decisions within organisations, not simply coming up with additional prescriptive rules.[108]

**56** This view is not shared equally across industry, however. Some industry players see a certain value in including PbD within the framework, at least to a certain extent,[109] so long as it does not mandate 'technological outcomes' or certification schemes.[110] The main tenor of the ICT industry remains intact notwithstanding: self-regulation is to be preferred over mandated schemes. Government's role should be to provide incentives for their adoption.[111]

**57** Data protection authorities for Canada, Germany, the UK and the EU, as well as the FTC in the US, have been clear that PbD is a concept that needs to be encouraged and that is vital to the proper progress of technology that will respect the privacy rights of its users or beneficiaries. In fact, at the 2009 International Conference of Data Protection and Privacy Commissioners, a resolution was passed that PbD is an 'essential component of fundamental privacy protection'. Not all DPAs, however, are univocal in their calls for *how* PbD ought to become part of legislative frameworks around the globe.[112]

**58** The 2010 'Conference of the Data Protection Commissioners of the Federation and the Länder'[113] of Germany suggested that the German data protection legislation[114] should in the future, among several other key elements, include provisions to integrate privacy into 'products and processes'.[115] This entails that not only would data controllers and data processors be legally responsible for PII but also manufacturers and designers, who would then be required to integrate data protection principles into their products. DPAs should then have the ability to audit, provide certificates of approval as well as publicly name violators. PbD was specifically mentioned as a requirement for data controllers to ensure that privacy principles were sufficiently integrated into systems before their deployment. If they were not, the data subject should then have the right to base claims on that omission.[116] That being said, it has also been acknowledged that technology-specific regulation might be a 'difficult task'[117] and that PbD might be more appropriate as a general principle across all technologies, rather than a term that is to be understood based on the technology it is attempting to regulate.[118]

**59** Generally, it is obvious that the German (federal and state) DPAs would favour a PbD principle that requires technological (i.e. PETs) and organizational elements at the design stage, rather than only organizational requirements. This view is shared by the European Data Protection Authority (DPA)[119], which has stated that along with including PbD as a general principle (in conjunction with the principle of 'accountability'), PbD should be regulated more specifically with respect to RFIDs, social networks and browser applications. The Article 29 Working Party has noted that as a fundamental right under Article 8 of the ECHR, PbD is to be 'embedded' into systems. Specifically, the Working Party calls for the incorporation of *binding* rules regarding not only security of data but data minimization, PETs, privacy-by-default settings, access controls and encryption and the ability of DPAs to enforce these provisions. These rules should bind system designers, producers and data controllers.[120] The Working Party was clear that a PbD in-principle-only approach would not be enough, and any European framework should include the possibility of regulations to mandate embedded design features.

**60** The UK Commissioner's views are more closely aligned with those of the US and industry than with the more prescriptive proposals of the Article 29 Working Party, the German Commissioner or now the EU Proposal. High-level principles and self-regulation are to be preferred over prescriptive or technology-specific regulations. In 'The Information Commissioner's response to the Ministry of Justice's call for evidence on the current data protection legislative framework',[121] the Commissioner noted that PbD should be included into the *Freedom of Information Act 2000*[122] as a principle but did not elaborate further on specific provisions, powers of the DPA or rights of the individual in this regard.

**61** In Canada, the views on PbD are, as with some other aspects of privacy protection, a middle ground between those of the continental European nations and the Anglo-Saxon (US and UK). The IPC views PbD primarily as a 'voluntary standard'[123] aimed at achieving a high-water mark of data protection and compliance. This, however, need not be the final extent to which PbD can be utilized to achieve excellence in privacy protection. Rather, the IPC is generally in favour of incorporating PbD into legislative frameworks but 'takes no sides'[124] in the debate on what legislated PbD requirements should ultimately look like – that is, whether PbD needs to be regulated so that certain technological measures are mandated or whether organizational requirements would suffice. The Canadian Commissioner's Office similarly considers PbD a 'fundamental component of privacy protection' but has so far remained silent on whether or not *PIPEDA* should contain in-principle-only, technology-prescriptive or any PbD provisions at all.

**62** Notwithstanding this generally neutral approach to legislated PbD, the IPC does note the potential of regulating specific applications, as we have seen with the inception of the Smart Grid and the biometric identification system for the welfare application system in Ontario. Some private sector businesses share the Commissioner's view of having industry, DPAs and regulators work together to achieve best practices when it comes to designing systems, in

particular where sensitive data is processed in, for example, eHealth applications and smart-meters or smart appliances.[125]

**63** In a very recent publication of her office, Dr Cavoukian offered a draft legislative framework intended to provide a 'flexible but enforceable' approach to privacy protection.[126] The paper outlines current legislative initiatives and applications of PbD, not unlike this paper, in the US, EU and Canada as a precipitant to its proposed draft framework.[127] This draft is prescriptive in that it mandates a 'Privacy by design program', including specific elements of such a program,[128] but does not go as far as mandating specific and enforceable technological solutions. The proposition also does not suggest mandatory 'privacy-by-default' settings:

> Whenever reasonably possible, provide for that privacy protection automatically, so that no action is required for individual users or customers to protect the privacy of their personal information [...]

**64** This notwithstanding that privacy by default is a foundational principle of PbD. Perhaps in anticipation of the logical criticism, Dr Cavoukian writes:

> In *Privacy by Design*, Privacy as the Default is the ideal condition to strive for. However, currently, the industry standard of practice for online consumer marketing is opt-out. Privacy as the Default would require a shift to 'opt-in.' But an immediate shift to an opt-in model (which is the standard of practice for sensitive information, such as personal health information) could be both impractical and, perhaps, harmful to industry.
>
> As one of the 7 Foundational Principles, *Privacy as the Default must be read alongside the remaining principles.* The fourth principle of Full Functionality (Positive-Sum, not Zero-Sum), requires that *PbD* achieve a doubly-enabling, 'positive-sum' solution that provides a win-win result for both consumers and businesses – not one at the expense of the other.
>
> Taking into account the context involved – and context is key – it is possible to develop a two-step process for achieving the spirit of Privacy as the Default in situations where the existing industry standard of practice presents a barrier to achieving the principle directly, right from the outset.

**65** While reasonable, the above justification is not entirely satisfactory. That all principles ought to be read alongside one another is a fair statement, but six of the seven principles speak directly to the protection of personal data; only one, the positive sum principle, speaks to the balancing of interests between privacy and other relevant areas. The way it is described in this proposal, however, suggests that all six principles protecting information must be viewed in the context of one principle, essentially creating a two-tier system of the foundational principles, because all other principles do not require a side-by-side reading, as they naturally work together. This approach has never been advocated before and, arguably, would be a departure from what is commonly understood as PbD. At least, there is no evidence that such an interpretative approach has been taken by any other advocates of PbD, most notably Peter Schaar.

**66** Ann Cavoukian's proposal makes an appropriate distinction between sensitive and less sensitive PII, as well as organization size,[129] but missing is any and all mention of developers or manufacturers of technology being truly accountable for the systems they develop (from a privacy standpoint). This is an indication that the IPC's approach to PbD may be 'Canadian' but will draw its influences from the developments in the US rather than the EU. In fact, the proposal notes its influences as the Kerry-McCain Bill, as well as Massachusetts legislation, while failing to mention either the Article 29 Working Party or the German Commissioner's recommendations in this regard.

**67** Feasibility[130] aside, PbD may not have much teeth if the obligations start at the user end of the life cycle. The German Commissioner notes that PbD principles need to be incorporated into products and services if PbD is to reach its full potential.[131] The IPC's proposition is silent on remedies or enforcement processes, so one could presume that the proposition would fit into the existing framework existing in, for example, Canada's *PIPEDA* or other European legislation. It does provide specific and helpful guidelines and processes for organizations to follow as part of a PbD program.[132]

**68** For organizations, the additional administrative burden could be substantial, and it would require a major change for many organizations, at least from a North American perspective. For those organizations active in Europe, the EU Directive already requires notification requirements for all automated or partially automated systems that process PII.

**69** In Sweden, for example, the obligation[133] is as follows (Section 36 Swedish Personal Data Act):

> Processing of personal data that is completely or partially automated is subject to a notification duty. The controller of personal data shall provide a written notification to the supervisory authority before such processing or a set of such

> processing with the same or similar purpose is conducted.[134]

**70** Such notification requirements obviously make supervisory authority of a PbD program easier, but they would be a massive change for both Canadian organizations (as well as being questionable whether a conservative government would ever condone such requirements) and the regulator.

**71** Ultimately, the framework proposed by the Ontario Commissioner is straightforward and practicable. It presents a manageable middle ground between corporate flexibility and prescribed data protection technology standards, and may therefore prove to be attractive for lawmakers. The underlying rationale is surely one that will surface during the debate and consultation process surrounding the EU Proposal.

## D. Analysis

> Individuals may want cyberspace to protect their privacy, but what would push cyberspace to build the necessary architectures? Not the market. [...]. Collective Action must be taken [...] and collective action is just what politics is for.[135]

**72** It is clear that PbD is, no matter which stakeholders you consult in this debate, viewed as a valuable tool to a) protect data and privacy and 2) build trust in the systems, which is ultimately part of the commercial and political goal of furthering technology and its widespread use in society.

**73** In order to build PbD into data protection legislation, there are clearly open matters which would require swift resolution. First and foremost, a decision would need to be made as to the manner in which this is to be achieved. Does one follow the proposed US road of organizational requirements, self-regulation or at best an in-principle-only mention in legislation or, alternatively, should PbD become an explicit integral part of law and mandate technology and standards? Or should PbD become part of *PIPEDA* or any other Canadian law at all?

**74** With the current government, it is highly unlikely that the Canadian federal framework will be adjusted to incorporate PbD any time soon. As noted, Bill C-12 includes nothing of the kind. However, if the EU Proposal moves forward to include prescriptive PbD requirements, Canada may find its hand forced to follow suit, at least incrementally.[136] Then the Canadian approach might very well be one that is firmly planted in the middle between the US and European ideas of PbD. The proposal by the IPC takes elements of both approaches into consideration. The problem, however, is that divergent approaches in this regard may not be very useful, given the borderless nature of modern computing. In the best-case scenario (from a privacy compliance perspective), an international company would adhere to the strictest standard, but given that the systems approach to legislated PbD requires all actors in the supply chain of the technology to embed PbD, this may become a very real practical problem. A European company could not easily source a system from the US if different legislative requirements applied to the technology and its application.

**75** The question of how older systems would be treated would also arise. The Ontario Commissioner is advocating 'privacy by re-design',[137] and it is not clear how this would fit into the legislative framework. Notwithstanding the wide array of open questions with respect to PbD and its appropriate implementation, it is quite apparent that privacy experts view it necessary to consider and embed data protection at the design stage to protect the fundamental right that is privacy. For certain applications this would include specific technological guidance for developers and data controllers without which the system could not be implemented. Whether these applications should include those mentioned in the Article 29 Working Party recommendation and in the EU Proposal may be a source for future research, but from the examples of the Smart Grid, ELENA and the biometric recognition application it is clear that there are systems that require specific solutions at their design stage such as encryption technologies, advanced cryptography in identification verification and privacy-by-default.

**76** An item of particular interest would be whether the assessment of a system according to PbD principles could lead to outright prohibition. A 'prior checking'[138] requirement already exists under the EU Directive (Article 20). France, for example, has translated this requirement into an explicit 'no-go' or prior authorization statement for systems processing certain categories of sensitive data. These categories include systems where biometric or genetic data is processed as well as corporate whistleblowing systems (as applications processing potentially incriminating data or containing information could have adverse effects on the career of employees).[139]

**77** Canadian federal and provincial legislation does not require notification to the authorities of systems processing PII regardless of any sensitivity. Privacy Commissioners could therefore not *prevent* a system from being deployed based on, for example, insufficient privacy design. However, via the accountable-person requirement, *PIPEDA* indirectly could prevent a system from being deployed if the accountable person was not convinced that the system complies with *PIPEDA*. If PbD formed an explicit part of the legislation, the accountable person would need to ensure that any system took privacy considerations into account at the

design stage before allowing it to go live. If the legislator provided concrete guidance on how this is to be achieved for particular potentially intrusive systems,[140] it would allow for the accountable person to benchmark more precisely. Failing to do so could then be the source of an enforceable complaint.

**78** What the foregoing analysis makes clear is that compliance with PbD could potentially become complex, resource-intensive and expensive. If organizations are complaining now about the minefield that is privacy law, PbD clearly will not make it any easier. For that reason regulators must find ways to use PbD to ameliorate the appropriate risks while not focusing solely on harm and risk. Recall that data protection can also be about democratic rights and the right to determine what is done to one's information. Additionally, seemingly non-sensitive information can in the aggregate become just that.

**79** Going forward, regulators must take a clear position on the importance of PbD regarding the protection of privacy. To accomplish this, PbD must first become an explicit principle of privacy law. Secondly, where the natureof the systems and sensitivity of the datademands, specific technological requirements should be legislated on top of general principles. Making PbD an explicit part of legislation only may be an important first step but would likely not be enough to ensure the desired level of protection, not to mention the fact that in-principle only would perhaps not even be a significant change from the current framework, at least that of the EU.

## E. Conclusion

**80** The speed at which information is being moved into digital environments and from manual to automatic processes surely requires a re-thinking of how information about individuals is collected, stored, used and then protected in these novel environments. PbD as a concept is attractive in this regard as its aim is to prevent rather than mitigate harm to PII. Instead of focusing on patching systems when data is already at risk, its focus lies in designing the architecture of the system in a privacy-respective manner. Of course, this approach is not always feasible as many organizations use systems that have been built and developed over time, long before PbD was a term of art or even long before omnibus privacy legislation existed in the EU, Canada or elsewhere. In other words, whatever the reach of PbD will be in the future, systems will require on-going privacy patches. For PbD to have the required punch, however, it needs to be explicitly mentioned in privacy legislation as well as prescribing technology-specific solutions where required. It is not enough to have PbD as an organizational best practice. This especially holds true for Canada where law does not require notification of PII processing to Information Commissioners (or explicitly to the accountable person) and systems could therefore go live without having been vetted from a design perspective. PbD is too important and effective from a data protection standpoint to stand at the periphery of a legislative framework. It should be at the core.

**81** Most importantly, any legislation would need to include a process through which a system or product could be prevented from going live until it is sufficiently data protective. This must be a part of the framework in the private sector. For this to work properly, before putting a system into operation, organizations would need to submit a proposal for how the system will process personal data and for what purposes. This is where a DPO can add significant value and accountability without the organization having to communicate directly with the authorities. Some organizations are already following this best practice and, as we have seen with ELENA,[141] the application of PbD principles can lead to the abandonment of a data processing application. In the public sector, these large projects are well-known before becoming operational, but in the private sector this is obviously not always the case. Companies can design or use applications that do not have adequate protection in their architecture. The public may only know about these systems when it is too late, when personal data has been lost on account of a breach, misappropriation or leak. Again, an accountable DPO (as stated in the EU Proposal) would be a valuable link between the organization and the law to ensure that systems are designed and used compliantly. For PbD to make any sort of real difference in the way that personal data is protected, every actor in the life cycle will need to be accountable for their systems and technologies from a privacy protection perspective. Products and applications need to be brought to market with PbD embedded from conception to finalization, and organizations need to use these products to design systems that follow those same principles. It is the regulator's mandate, however, to ensure that legislative requirements are sufficiently clear and that their adherence can be tracked (and enforced). Notwithstanding this obligation, the argument that any lack of clarity on the specific meanings of PbD in every context should mean that its legislative adoption should not be encouraged, cannot stand where the right sought to be protected is as fundamental as the right to informational self-determination and to be let alone.

■

* David Krebs is currently working as Compliance Counsel for an international company located in Sweden. This article was written as part of his LL.M. at Stockholm University. The paper was presented at the "1st International Research

Forum on Law and ICT/IP" on7th / 8th of November 2012 at Georg-August-Universität in Göttingen, Germany. The Colloquium is an annual event and provides the opportunity for young researchers to present the results of their scientific work and obtain valuable feedback from senior academics and practitioners in the field of ICT and IP Law.

1 This term stems from German privacy law ('*informationelle Selbstbestimmung*'). For more on the cultural aspects of global privacy laws, see Lee Bygrave, 'Data Protection in a Global Context', in *Scandinavian Studies in Law Volume 47: IT Law,* Peter Wahlgren (ed), (Stockholm: 2004) [Bygrave] and Lee Bygrave, 'Privacy and Data Protection in an International Perspective', in *Scandinavian Studies in Law Volume 56: IT Law*, Peter Wahlgren (ed), (Stockholm: 2010) [Bygrave 2].

2 See Samuel Warren and Louis Brandeis, 'The Right to Privacy', (1890) 4 Harv. L. Rev. 193.

3 The terms 'personal information' and 'personal data', stemming from Canadian and EU law, respectively, will be used synonymously, as will the EU term 'processing' referring to the Canadian terms collection, use and disclosure.

4 Facebook serves as a prime example of where privacy considerations have been added bit by bit but were never part of the original design. On the contrary, the design was such that would allow maximum sharing with very few automatic restrictions on data transfers.

5 Privacy By Design, online: http://www.privacybydesign.ca/about/principles/.

6 S.C., 2000, c.5.

7 *PIPEDA* is Canada's federal private-sector legislation. It applies to all commercial activities involving PII as well as to employee information for federally regulated organizations (e.g. banks). In provinces that have 'substantially similar' protections, *PIPEDA* does not apply other than to federally regulated undertakings or in relation to cross-border activities.

8 EC, Commission Directive 95/46/EC on the *protection of individuals with regard to the processing of personal data and on the free movement of such data*, 1995 O.J. (L 281) 31–39 (EC) (Oct. 24, 1995), online: EurLex http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML [EU Directive].

9 *Ibid.*

10 EC, *Proposal for a Regulation of the European Parliament and Council on the Protection of individuals with regard to the processing of personal data and the free movement on such data (General Data Protection Regulation)*, 2012/0011(COD) [EU Proposal].

11 US, Bill S., *Commercial Privacy Bill of Rights Act of 2011*, 112th Cong., 2011.

12 Generally described as '[...] technologies designed to give the user more control' over personal information. For example, such PETs would allow a user to retain her online anonymity. Code 2.0, *supra*, at 223-224.

13 An example of this would be the bilateral adoption of breach notification requirements. See e.g. 'Top 11 Privacy Trends for 2011', Ernst & Young, online: www.ey.com/GL/en/Services/Advisory/IT-Risk-and-Assurance/Top-11-privacy-trends-for-2011---2--Breach-notification-requirements.

14 Bygrave, supra, at 340.

15 Dr Ann Cavoukian, 'Privacy by Design in Law, Policy and Practice: A White Paper for Regulators, Decision-makers and Policy-makers' (August 2011), Information and Privacy Commissioner of Ontario, available at: www.privacybydesign.ca [PbD Whitepaper].

16 Author's note: While this paper is written from a Canadian perspective, the aim is to approach PbD in a manner that takes other laws and viewpoints into account and therefore any recommendations are targeted not only at Canadian federal legislation.

17 Lawrence Lessig, *Code Version 2.0,* (New York, 2006) at 6 [Code 2.0].

18 For such an analysis, see Avner Levin and Mary Jo Nicholsen, 'Privacy Law in the US, EU and Canada: The Allure of the Middle Ground', (2005) University of Ottawa L.& T. J. 357.

19 For example, Brazil, Chile, South Africa, inter alia, see Byrgrave, *supra* at 341 -343.

20 EC, *Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms,* [1953], European Treaty Series No. 5.

21 1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

22 See *Hunter v. Southam*, 2 S.C.R. 145, 159-60 (1984).

23 Part I of the *Constitution Act*, 1982, being Schedule B to the *Canada Act* 1982 (U.K.), 1982, c. 11.

24 'The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.' For a discussion on the nature of this right regarding modern communications, see Daniel Solove, *The Digital Person* (New York: New York University Press, 2004), cited in Dr Ann Cavoukian, *Privacy and the Open Networked Enterprise,* (2006).

25 In an Opinion to the Privacy Commissioner former Supreme Court Justice La Forest notes that: 'Determining whether individuals have a reasonable expectation of privacy in a given context is a nuanced, contextual, and fundamentally normative enterprise.' Gerard La Forest, 'Opinion by Justice Gerard La Forest', (April 5, 2002), *Office of the Information and Privacy Commissioner*, available at http://www.priv.gc.ca/media/nr-c/opinion_020410_e.cfm.

26 See William MacKinnon, 'Do We Throw Our Privacy Rights Out With the Trash? The Alberta Court of Appeal's Decision in *R. v. Patrick'*, (2008) 46 Alta. L. Rev. 225 [MacKinnon].

27 See Levin, *supra*.

28 [1988] 2 S.C.R. 417 at para. 34.

29 R.S., 1985, c. P-21.

30 Alberta, British Columbia, Ontario and Quebec have private sector legislation, and most other jurisdictions have public and sector-specific legislation, such as in Saskatchewan, Manitoba, Ontario and Alberta where legislation protecting personal health information is in force.

31 See *Byrgave*, *supra*, at 326-331.

32 Levin, *supra*, at 392.

33 See Levin, *supra*, and Lanois, *supra*.

34 These tracking devices have a range of applications and can be found in consumer goods and used by retailers to track the supply chain, but also for highway tolls and in public libraries. The privacy implications stem from the fact that these tags can collect, store and transmit PII as well as track locational data of the device (and therefore, potentially, the individual associated with a device containing an RFID). For more on RFIDs and a detailed analysis of RFIDs and *PIPEDA*, see Teresa Scassa et. al, 'An Analysis of Legal and Technological Privacy Implications of Radio Frequency Identification Technologies', (April 28, 2005), University of Ottawa, online: http://commonlaw.uottawa.ca.

35 Information and Privacy Commissioner of Ontario, 'Privacy by Design: The 7 Foundational Principles, (August 2009, revised January 2011), Information and Privacy Commissioner of Ontario, online: http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf.

36 Dr Ann Cavoukian, 'The 7 Foundational Principles', Office of the Information and Privacy Officer, online: www.ipc.ca.

37 See a complete list of all ambassadors at Privacy by Design, online: http://privacybydesign.ca/ambassadors/individuals/page/3/.

38 Peter Schaar, 'Privacy by Design', (April 1, 2010), Springerlink, online: http://www.springerlink.com.

39 A good example of the win-win or 'positive-sum' approach advocated by the Ontario Commissioner's Office (IPC) is the use of advanced cryptography for user identification. Contrary to the often-advocated theory that security and privacy consideration are intrinsically at odds with one another – misconceptions often rooted in an ignorance of the modern technologies – modern technology can in fact cater to both sides of the coin. In this example, use is made of a trusted third party who, during a one-time certification stage, issues separate randomly generated ID tokens to be used vis-à-vis certain service providers requiring secure identification, and embeds all of these tokens (contained in a smart chip) with an invisible 'master' ID key. Where required, the IDs can be shared across service providers without any one party knowing or being able to trace the IDs back to the individual. Information is always a) controlled by the individual and b) limited to the identification parameters that the service provider requires. See Stefan Brands, 'Secure User Identification Without Privacy Erosion', (2006) University of Ottawa L.& T. J. 205 [Brands].

40 Such as the secure ID tokens described in Brands, *supra*.

41 See Bygrave 2, *supra*, at 169, for a comparative analysis of the cultural aspects underlying privacy laws.

42 Cavoukian, Ann, PhD, *Privacy by Design in Law, Policy and Practice: A Whitepaper for Regulators, Decision-makers and Policy-makers*, (August 5, 2011), online: http://privacybydesign.ca.

43 Seda Gurses et al., 'Engineering Privacy by Design', (2011), Computers, Privacy and Data Protection (CPDP 2011 Conference) available at http://www.cosic.esat.kuleuven.be/publications/article-1542.pdf [Gurses].

44 *Ibid* at 5.

45 Smart Grid Canada, available at http://sgcanada.org/smart-grid/what-is-a-smart-grid/: 'allows utilities to distribute conventional and renewable power to consumers more efficiently, reliably, safely and economically. It integrates two-way digital communication technology that analyzes, monitors and streamlines the system to maximize throughput, while promoting and enabling a reduction of overall energy consumption.'

46 Dr Ann Cavoukian, 'Privacy by Design: Achieving the Gold Standard in Data Protection for the Smart Grid', (2010), Privacy by Design, online: http://www.ipc.ca.

47 Sebastian Knab et. al. 'Smart Grid – the Central Nervous System for Power Supply', (2010), *Scientific Series of the Innovation Centre Energy at the Technische Universität Berlin, Vol. 2, University Press, Berlin, Germany,* available online at SSRN, http://ssrn.com/abstract=1531655.

48 BC Hydro, online: http://bchydro.com/energy_in_bc/projects/smart_metering_infrastructure_program/smart_meter_installation.html.

49 Knab, *supra*.

50 'Monitoring a consumer's energy use in near real time, a smart meter delivers incremental consumption data and pricing.' From Smart Grid Canada, *supra*.

51 IT Law Wiki, available at http://itlaw.wikia.com/wiki/Smart_appliance: 'A smart appliance is an appliance that may be configured to communicate information directly to the utility operator for efficient and more productive use of electricity.'

52 Elias 'Smart Metering and Privacy: Existing Law and Competing Policies', (2009), *University Colorado Law School – CEES*, Working Paper Series, available at SSRN, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1462285. These include services like energy efficiency monitoring and home load management.

53 *Ibid*, at 12.

54 National Institute of Standards and Technology, 'NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0', (January 2010) at 118-119.

55 *Ibid*.

56 Information and Privacy Commissioner of Ontario, 'Operationalizing Ontario's Privacy By Design: The Ontario Smart Grid Case Study', (February 2011), Privacy by Design, available at http://www.ipc.on.ca/images/Resources/pbd-ont-smartgrid-casestudy.pdf [Smart Grid Case Study].

57 In British Columbia, for example, meter installations began in July 2011, and it is estimated that by the end of 2012 all residential customers will have their meters upgraded to smart meters.

58 Ontario Smart Grid Forum, 'Modernizing Ontario's Electricity System: Next Steps. Second Report of the Ontario Smart Grid Forum', (May 2011, at 7-8).

59 For example, increasingly efficient and precise ways of collecting meter data for precise load forecasting.

60 See Smart Grid Case Study at 16.

61 'Privacy Concerns Surround Ontario's Smart Grid Plan', (11 May 2010), online: www.cbc.ca/news/technology/story/2010/05/11/cavoukian-privacy.html.

62 An electronic signature based on a qualifying certification agency's certificate. See Footnote 67 below.

63 Wikipedia, 'ELENA-Verfahren', Wikipedia, available at http://de.wikipedia.org/wiki/ELENA-Verfahren, last accessed on 15 October 2011.

64 Peter Schaar, *supra* note 27.

65 Press Release, 'ELENA Verfahren wird eingestellt' (translated: ELENA process will be discontinued), Bundesministerium für Arbeit (German Ministry of Labour), online: BMWi, http://www.bmwi.de/BMWi/Navigation/Presse/pressemitteilungen,did=424742.html.

66 Defined as 'an advanced electronic signature based on a qualified certificate and created using a secure signature creation device' in Cecilia Magnusson Sjöberg & Anna Norden, 'Managing Electronic Signatures', *Scandinavian Studies in Law Vol. 47: IT Law*, ed. Peter Wahlgren, (Stockholm: 2004), at 84. An advanced electronic signature is one created using so-called Public Key Infrastructure, which ensures the integrity and authenticity of a signature using one private and one public key and a certification authority 'vouching' for the link between the private key and a flesh and blood individual.

67 'Bundesregierung beerdigt Arbeitnehmer Datenbank', T-Online, online: http://wirtschaft.t-online.de/elena-bundesregierung-beerdigt-arbeitnehmer-datenbank-elena-/id_48125142/index.

68 In that recommended changes were built into the DNA of the system and processes.

69 See Dr Ann Cavoukian, 'Privacy and Biometrics: An Oxymoron or Time to Take a 2nd Look?', (1998), Information and Privacy Commissioner Ontario, online: http://www.ipc.on.ca/english/Resources/Presentations-and-Speeches/Presentations-and-Speeches-Summary/?id=98: The City of Ontario at the time had been worried about citizens applying for benefits on multiple occasions on the same bases through the use of multiple identities.

70 *Social Assistance Reform Act, 1997, O.Reg. 226/98*.

**71** 1997, S.O., c-25, Schedule A.

**72** 1997, S.O., c-25, Schedule B.

**73** *Ontario Works Act, s.74(3).*

**74** This is the key difference between sensible security or privacy protective measures and PbD, which takes these sensible measures, forces their application on the design of the system and makes it a requirement that is done alongside the other technical design stages of a system.

**75** Lawrence Lessig, *Code, 2.0, supra*, at 232.

**76** It is an example of a way to satisfy Principle 4.7.1 (see e.g. PIPEDA Case Summary #2003-185) of *PIPEDA* but not an explicit requirement.

**77** In British Columbia, for example, the private-sector act is intended to cover the health sector.

**78** This statement must be viewed in the context of a comparison with the landscape in the EU. There are indeed differences within Canada as to how PII may be used, collected and disclosed, but the manner in which the private sector is regulated by *PIPEDA* and provincial legislation is cohesive in that common principles and a common culture underlie the regulations. See e.g. David Krebs, 'Regulating the Cloud: A comparative analysis of the current and proposed privacy frameworks in Canada and the European Union', (to be published in the Spring 2012 Volume of the CJLT).

**79** Canadian Standards Association, online: http://www.csa.ca/cm/ca/en/privacy-code/publications/view-privacy-code. The CSA is the Canadian agency responsible for the collection and publishing of applicable standards in Canada.

**80** *PIPEDA* Report of Findings #2011-001. See also discussion in PbD Whitepaper, *supra* at 27. The Commissioner instigated the complaint for data collected without knowledge or consent of the individual, beyond the purposes required and without identifying and disclosing the purposes of the data collection by way of Google's Street View cars.

**81** Principle 4.1.

**82** Ss. 15-16.

**83** 1st Sess., 41st Parl., 2011.

**84** In order to be able to transfer data outside of the EU, the recipient country must have 'adequate' data protection laws (Art. 25 EU Data Protection Directive). Currently, *PIPEDA* is considered 'adequate', but this could change if the two frameworks do not continue to be similar in their protections.

**85** Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002.

**86** Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006.

**87** Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009.

**88** 1998:204 PuL (Swedish Personal Data Act) [Swedish Personal Data Act].

**89** Cecilia Mangusson Sjöberg et al., *Rättsinformatik*, (Studentlitaratur: Lund, 2011) at 31.

**90** (UK), 1998, c. 29.

**91** E.g. Privacy by Design, *supra*.

**92** One must remember at this point that under civil law, recitals and even preparatory works have a higher legal status than under Canadian common law. In Sweden, for example, courts often consider these to carry a great deal of weight. See Samuel Engblom, *'Regulatory Frameworks and Law Enforcement in New Forms of Employment: National Report: Sweden'*, Report to the XIX World Congress of Labour and Social Security Law (Sydney 2009), TCO, online: http://www.tco.se/56e6d647-e578-41dc-947f-2775c4f8fcfe.fodoc.

**93** WP 168.

**94** Under EU law, a 'controller' is the legal person that identifies and determines the purposes of the PII that is processed. A 'processor' is a legal person that may process PII under the direction of the controller. Separate legal obligations apply depending on this determination. See definitions within EU Directive, *supra*.

**95** WP 168 at 13.

**96** PbD regulation at 19.

**97** EC, *Proposal for a Regulation of the European Parliament and Council on the Protection of individuals with regard to the processing of personal data and the free movement of such data (General Data Protection Regulation)*, 2012/0011(COD) [Proposal].

**98** The current Directive states that 'Member States shall provide that the controller or his representative, if any, must notify the supervisory authority referred to in Article 28 before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes' unless a DPO is appointed who maintains a register of systems or 'where, for categories of processing operations which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects, they specify the purposes of the processing, the data or categories of data undergoing processing, the category or categories of data subject, the recipients or categories of recipient to whom the data are to be disclosed and the length of time the data are to be stored.'

**99** Arts. 35 – 37.

**100** This would not be new for all Member States. Sweden, for example, already has a similar requirement.

**101** US, Bill S. 1, 112th Congress, 2011.

**102** See 'Joint Statement on Commercial Privacy Rights', *Ebay Mainstreet*, (11 April 2011), online: Ebay Mainstreet, http://www.ebaymainstreet.com/files/Joint-Statement-on-Commercial-Privacy-Bill-of-Rights-April-12-2011.pdf.

**103** 'Consumer Groups Welcome Bipartisan Privacy Effort, But Warn Kerry-McCain Bill Insufficient to Protect Consumers' Online Privacy', *Consumer Watchdog* (12 April 2011), online: Consumer Watchdog, http://www.consumerwatchdog.org/newsrelease/consumer-groups-welcome-bipartisan-privacy-effort-warn-kerry-mccain-bill-insufficient-pr.

**104** 15 U.S.C. § 45.

**105** Consent Decree, Agreement containing consent order, File No. 102 3136 http://www.ftc.gov/os/caselist/1023136/110330googlebuzzagreeorder.pdf.

**106** Federal Trade Commission, 'Protecting Consumer Privacy in an Era of Rapid Change', December 2010, online: http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

**107** See e.g. World Federation of Advertisers (WFA), *Submission to the Consultation on the Commission Communication on 'A comprehensive approach on personal data protection in the European Union'* [COM (2010) 609/3], European Commission, online: http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm.

**108** Vodafone, *Vodafone's Response to the Consultation on the Commission Communication on 'A comprehensive approach on personal data protection in the European Union'* [COM (2010) 609/3], European Commission, available at http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm at 6.

**109** See e.g. Microsoft, *Submission to the Consultation on the Commission Communication on 'A comprehensive approach on personal data protection in the European Union'* [COM (2010) 609/3], European Commission, available at http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm: 'Microsoft supports an industry-wide PbD obligation applicable to the ICT industry to take account of privacy principles, including notions of data

minimisation, transparency, user control, use limitation, and related principles, in the development and deployment of new technologies. As with accountability generally, it is important that we reach a common understanding of what PbD entails, however. PbD obligations should not take the form of design mandates or technology preferences, for example. Indeed, it would be undesirable for privacy rules to dictate specific technological outcomes – including 'privacy by default' – which will only impede the development of new technologies without guaranteeing stronger privacy protections. PbD obligations for any given technology should be proportionate to the privacy risks to the consumer; program assurance should place an emphasis on trustworthy internal checks and balances and limit reliance on third party audits and mandatory privacy certifications, which often impose significant costs with little concomitant benefit (to the extent external validation is necessary, it should be reasonable in scope and affordable); and there must be clear benefits for those companies that submit to higher levels of validation to demonstrate trustworthiness.' Also see European Networks, Response to *the Consultation on the Commission Communication on 'A comprehensive approach on personal data protection in the European Union'* [COM (2010) 609/3], European Commission, available at http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm.

**110** *Ibid*.

**111** See e.g. Facebook, *Submission to the Consultation on the Commission Communication on 'A comprehensive approach on personal data protection in the European Union'* [COM (2010) 609/3], European Commission, available at http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm.

**112** I would contend that this is at least partially attributable to the notion of privacy *rights* and the differences across cultures. For more on this topic, see Bygrave, *supra*.

**113** Conference of the Data Protection Commissioners of the Federation and the Länder, *Modern Data Protection for the 21st Century,* The Data Protection Commissioner of Baden-Württemberg (18 March 2010) [2010 Conference].

**114** *Bundesdatenschutzgesetz*, (BGBl.I 1990 S.2954) [BDSG].

**115** 2010 Conference, at 6.

**116** *Ibid* at 9.

**117** Opinion of the Federal Commissioner for Data Protection and Freedom of Information, email correspondence with David Krebs (5 August 2011).

**118** *Ibid*, opinion of the German DPA.

**119** European Data Protection Supervisor (Peter Hustinx), *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – 'A comprehensive approach on personal data protection in the European Union'*, 14 January 2011 at para 114.

**120** Art. 29 Data Protection Working Party, *The Future of Privacy*, 02356109/EN, WP168 (01 December 2009) [WP 168].

**121** Available at Information Commissioner's Office, online: http://www.ico.gov.uk/about_us/consultations/consultation_responses.aspx.

**122** 2000 c. 36.

**123** PbD Whitepaper, *supra*, at 21. These voluntary codes can, of course, be either in-principle-only or technology prescriptive.

**124** Email correspondence with Gail Puder, OPC, (April 2011).

**125** See e.g. General Electric Company, Submission *to the Consultation on the Commission Communication on 'A comprehensive approach on personal data protection in the European Union'* [COM (2010) 609/3], European Commission, available at http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm at 10.

**126** PbD Whitepaper, *supra*.

**127** It was published before the EU Proposal was finalized and did not consider its implications.

**128** 'A comprehensive *Privacy by Design program* must include the following elements: (1) An organization shall establish a *Privacy by Design* leader and/or team by identifying the appropriate directors, officers, and managers responsible for developing, maintaining, implementing, and updating proactive *Privacy by Design* processes and practices; (2) Proactive *Privacy by Design* processes and practices shall: (A) Apply to the design and architecture of infrastructure, IT systems, and business practices that interact with or involve the use of any personal information; (B) Describe each of the core purposes served and main functions delivered by those infrastructures, systems and practices, including but not limited to the provision of security and the protection of privacy in personal information; (C) Incorporate data minimization and provide the highest degree of privacy protection for personal information possible while serving the other core purposes and delivering the other main functions; (D) Provide this degree of privacy protection by employing the maximum feasible means needed to ensure the security, confidentiality, and integrity of personal information throughout the lifecycle of the data, from its original collection, through to its use, storage, dissemination, and secure destruction at the end of the lifecycle; (E) Whenever reasonably possible, provide for that privacy protection automatically, so that no action is required for individual users or customers to protect the privacy of their personal information; (F) Ensure that infrastructure, IT systems, and business practices that interact with or involve the use of any personal information remain reasonably transparent and subject to independent verification by all relevant stakeholders, including customers, users, and affiliated organizations; and (G) Emphasize the design and maintenance of user-centric systems and practices, including strong privacy defaults, appropriate notice, and other user-friendly options.

**129** 'Each organization shall, in a manner proportional to the organization's size, scope, and resources and the size, type, and nature of the *personal information* that it collects, implement a comprehensive *Privacy by Design* [...]'.

**130** This method of regulating raises a number of concerns. First, to what standard will organizations be held and how enforceable will this standard be? Further, how will the separate but connected obligations of system designers, purchasers and data controllers be enforced (that is, to what extent will a data controller be accountable for a designer's adherence to the systems)? External certifications and internal control processes will surely play a role in this, but given the complexity of the technology today, data controllers may well have to rely on system designers to guarantee that certain principles are adhered to. For example, when it comes to complex encryption technologies to ensure secure authentication and access controls, it may not be feasible to require the business to understand the algorithm underlying a Public Key Infrastructure encryption tool, but only a certificate that the algorithm meets the requirements of data protection laws.

**131** Peter Schaar, *supra* note 27 at 1.

**132** 'In support of a comprehensive *Privacy by Design* program, an organization must: (1) Provide appropriate privacy and security training to its employees; (2) Implement a system for tracking all projects that regularly collect, use or store personal information; (3) Require project leaders to draft, maintain, submit and update Privacy Design Documents for all projects in order to help ensure product, program or service teams assess the privacy impact of their products, programs and services from inception through launch; and (4) Assign an internal audit team to conduct periodic audits to verify the

completion of selected Privacy Design Documents and their review by the appropriate managers.'

**133** Although Sweden is not a jurisdiction that has traditionally enforced provisions such as the above, the PuL contemplates a fine or imprisonment of up to two years for grave breaches (Section 49).

**134** Translation taken from Swedish Government Offices English language version of the Act, online: http://www.sweden.gov.se/content/1/c6/01/55/42/b451922d.pdf.

**135** *Code 2.0*, *supra* at 232.

**136** The Proposal maintains the current restrictions (Art. 25 of the EU Directive, supra) on data transfers to countries that do not have 'adequate' legislation in place. Canada is currently considered 'adequate' and transfers to Canada can be conducted from EU Member States without any other special exemptions (BCRs, mandatory contractual clauses),, but it could be that in order to maintain this classification, Canada would need to move forward in the same manner.

**137** See Privacy by Design, online: http://privacybydesign.ca.

**138** 1. Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof. 2. Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official, who, in cases of doubt, must consult the supervisory authority. 3. Member States may also carry out such checks in the context of preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which define the nature of the processing and lay down appropriate safeguards.

**139** *LOI n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés* (Art. 25).

**140** E.g. social networking, RFID, Smart Grid.

**141** In France, a whistleblowing system was just recently struck down even despite its prior authorization from the French DPA (the 'CNIL'). See Hogan Lovells, online: http://www.hldataprotection.com/2011/10/articles/international-eu-privacy/french-court-of-appeals-reject-companys-whistleblower-system-despite-cnil-approval/.

# On the Role of Copyright Protection in the Information Society

## Anti-ACTA Protests in Poland as a Lesson in Participatory Democracy

by **Katarzyna Gracz***
Phd Candidate at the Department of Law, European University Institute, Florence

**Abstract:** In January 2012, Poland witnessed massive protests, both in the streets and on the Internet, opposing ratification of the Anti-Counterfeiting Trade Agreement, which triggered a wave of strong anti-ACTA movements across Europe. In Poland, these protests had further far-reaching consequences, as they not only changed the initial position of the government on the controversial treaty but also actually started a public debate on the role of copyright law in the information society. Moreover, as a result of these events the Polish Ministry for Administration and Digitisation launched a round table, gathering various stakeholders to negotiate a potential compromise with regard to copyright law that would satisfy conflicting interests of various actors.

This contribution will focus on a description of this massive resentment towards ACTA and a discussion of its potential reasons. Furthermore, the mechanisms that led to the extraordinary influence of the anti-ACTA movement on the governmental decisions in Poland will be analysed through the application of models and theories stemming from the social sciences. The importance of procedural justice in the copyright legislation process, especially its influence on the image of copyright law and obedience of its norms, will also be emphasised.

**Keywords:** Copyright; Compliance; ACTA; Sociology of Law



Recommended citation: Katarzyna Gracz, On the Role of Copyright Protection in the Information Society, 4 (2013) JIPITEC 21, para. 1.

## A. Introduction

1 In January 2012, Poland witnessed massive protests, both in the streets and on the Internet, opposing ratification of the Anti-Counterfeiting Trade Agreement,[1] which triggered a wave of strong anti-ACTA movements across the whole of Europe. In Poland, these protests had further far-reaching consequences, as they not only changed the initial position of the government regarding the ratification of the Treaty but also actually started a public debate on the role of copyright law in the information society. Moreover, as a result of these events, the Polish Ministry for Administration and Digitisation launched a round table, gathering various stakeholders to negotiate a potential compromise with regard to copyright law that would satisfy conflicting interests of various parties to the dispute. This round table was the beginning of the wider social consultations with academia, non-governmental organisations, industry and interested individuals on the shape that the potential reform of the Polish law in general (not only intellectual property law) should take to be able to adequately meet the expectations of the information society. The consultations, apart from intellectual property law, focused on the new Internet business models,

protection of privacy, digital exclusion/integration and the meta topic, i.e. the issues of successful formula for social consultations in the digital environment.[2]

2 In general, it might be stated that the Polish government learned an important lesson during the anti-ACTA protests and realised that recent changes, which took place in Polish society due to the information revolution, changed the political climate in the country and the rules of the political game, in which civil society must be taken into consideration in the process of ruling and setting the goals of governmental policies.[3] The anti-ACTA protests proved also that freedom of Internet, including protection of free speech and wide access to knowledge and art in the digital environment, are important values in Polish society, which should shape the governmental plans and strategies. Moreover, the role of the Internet as a successful communication tool in the relations between the state representatives and the civil society was emphasised.

3 Change in the governmental position on the ACTA treaty was a trigger for the formulation of the wider, multi-dimensional policy with regards to the problems of the digital environment, in which the Polish government decided to base its decisions on wide social consultations with many stake holders. This new direction taken by the Polish government, as a result of the anti-ACTA protests, should be interpreted as supporting open Internet, especially various safeguards of the freedom of speech in the digital environment, net-neutrality and the idea of the Internet as a global public good.[4] The anti-ACTA movement in Poland resulted in a very courageous approach by the government that differs greatly from the current trends in the European and Northern American arena that seems to favour corporate benefits over the public interest.

4 This contribution will endeavour to describe and analyse the characteristics of the anti-ACTA movement and explain its extraordinary influence on the governmental decisions in Poland through the application of models and theories stemming from the social sciences. To facilitate reading, this article has been divided into two parts. The first is devoted to the description of the anti-ACTA phenomenon, whereas the second puts the protests in the wider context of the current crisis of copyright norms in the digital environment and evaluates actions taken by the Polish government in reaction to public discontent as a positive step on the way to restoring lost respect for copyright regulations.

## I. The anti-ACTA protests in Poland

5 In January 2012, all of Europe[5] witnessed massive protests, both in the streets and on the Internet, opposing the ACTA agreement, as a result of which ratification of the Treaty by the European Union has halted.[6] The anti-ACTA movement started in Poland and it was also here that the protests lasted the longest and had the furthest-reaching consequences. The protest started first in the virtual world after media informed the Polish society about the government's willingness to sign the Treaty. On the 21st of January, a number of Polish governmental websites, including the official sites of the President, Prime Minister and the Parliament were shut down by the denial of service attacks. Shortly afterwards the protests in the streets started, which spread when the Polish ambassador to Tokyo signed the Treaty notwithstanding the clear objection of the general public.[7] It is estimated that around a hundred thousand people went to the streets of dozens of big cities and smaller towns in Poland to show their objection to the ratification of the controversial treaty.[8] They stayed in the streets for long weeks, notwithstanding the extremely unfavourable weather conditions, when the temperatures were falling to as low as minus 20 degrees.

6 The intensiveness of the anti-ACTA protests has attracted the attention of many social scientists[9] as Poland has not witnessed such a social mobilisation since the collapse of the communist regime. Poles did not organise significant protests when the whole world was opposing the war in Afghanistan and Iraq. There was no "*Occupy Poland*" that was recognised as an influential social movement and Polish "*Indignados*" did not raise their voice in a manner similar to their counterparts in Southern Europe.

7 There are various explanations for the anti-ACTA phenomenon in Poland, ranging from the assertion that it was exactly this lack of earlier expression of discontent on the part of the society that led to the protests as they gave necessary vent to accumulated frustration[10], to the diagnosis that the secret negotiations on the Treaty and the unclear position of the Polish government triggered conspiracy theories and pushed people to protest even though they were not aware of the substance of the criticised legal act. The fact that the well-publicised protests against SOPA and PIPA took place only two days before the Polish government announced its willingness to sign the ACTA should also not be underestimated.

8 The reasons for this unprecedented rise of the Polish public opinion against the international treaty dealing with the complicated and technical regulations in the scope of intellectual property are multiple. Understanding the mechanisms that led hundreds of thousands of individuals to join the anti-

ACTA movement and protest in the streets in very unfavourable weather conditions requires, however, an analysis of the protesters' self-statements that can be reconstructed from the discourse covered in detail by the media.[11]

## 1. Why did they voluntarily freeze? On the reasons of the anti-ACTA protests.

**9** The analysis of the discourse presented in the media during the protests allows for the classification of various causes self-reported by the protesters, both individuals and organisations, which made them join the anti-ACTA movement. They might be divided into two general categories: reasons of *legal* nature and reasons of *extralegal* nature. The first category should be subdivided into two types: *legal* reasons of *material* and *procedural* nature.[12]

**10** The *material* reasons hereinafter are understood as referring to the provisions of the controversial treaty that might have led to changes in Polish law. The causes of *procedural* nature refer to the procedures that were applied in the process of negotiations and ratification of the ACTA treaty.

### a. Reasons of legal nature

#### aa. Legal reasons of material nature

**11** With regards to the causes of *material* nature, the protesters were afraid that ratification of the ACTA treaty might endanger access to knowledge and art in the digital environment, especially by changing the scope of the *permissible personal use clause* that has quite a liberal wording in current Polish copyright law as compared to other European regulations. They also pointed at the expressions used in Article 9 of the ACTA Treaty, which refers to damages for copyright infringement, warning that the concepts used in this provision stem from the Anglo-Saxon common-law copyright tradition and as such may drastically change the model used so far in Polish copyright law for determining the amount of damages in cases of copyright infringement.[13] The protesters stated that they were afraid of massive trials against the end-users, similar to the proceedings that have already taken place in the United States. They emphasised that such a practice is unknown so far in the Polish legal system and might also seriously endanger legal access to knowledge and culture if the individuals threatened with arbitrarily-determined and extremely high damages will fear acting even within the scope of their *permissible personal use*.[14]

**12** The representatives of the anti-ACTA movement also raised the argument that the regulations of the controversial treaty endangered freedom of expression on the Internet and the protection of personal data. They also argued that ratification of ACTA would allow for the introduction of the institution of a *private police* by granting power to private entities, such as ISPs and collecting societies, in the scope of enforcement in cases of copyright infringement, which would remain outside judicial control.

**13** They stated that ratification of the ACTA treaty would lead to the unacceptable situation in which private interests of the copyright-holders would be valued more highly than the fundamental rights of individuals (protection of privacy and freedom of speech) and the common public interest (access to knowledge and art and freedom of speech).

**14** It is worth mentioning that Polish Ombudsman and General Inspector for the Protection of Personal Data shared the above mentioned worries raised by the protesters in their official statements, in which they strongly advised against ratification of the ACTA treaty.[15]

#### bb. Legal reasons of procedural nature

**15** The reasons of *procedural* nature enumerated by the representatives of the anti-ACTA movement included secrecy of the negotiations of the Treaty on the international level, lack of adequate social consultations with all the stakeholders on the national level, lack of public discussions in the media before the ratification, and the atmosphere of hatching and conspiracy during the whole legislative process. Also these types of accusations against the government were acknowledged both by the Ombudsman and the General Inspector for the Protection of Personal Data. In her letter to the Prime Minister of 25th January 2012, the Ombudsman stated that the procedures applied both at the level of negotiations and ratification of the ACTA treaty were against the rule of law expressed in Article 2 of the Polish Constitution.[16]

### b. Reasons of extralegal nature

**16** Reasons of *extra legal* nature, i.e. postulates that did not directly refer to law, neither to its material nor to procedural aspects, could be described as political postulates of the leftist orientation that resonated very well with the earlier slogans of the *"Occupy"* and *"Indignados"* movements. The anti-ACTA protesters were formulating postulates against favouring corporate interests over public good. They were also promoting a liberal approach to access to knowledge and culture and protesting against globalisation and gradual monopolisation/oligopolisation of the creative industries by multi-national corporations, which in their opinion is leading to a decrease

in diversity on the cultural goods market. The protesters were also raising their voices against the aspirations of the American entertainment industry to impose American legal solutions on those outside the territory of the U.S.

## 2. The paradox of the anti-ACTA protests

**17** Paradoxically, when the protests commenced, the majority of the Polish copyright scholars unequivocally stated that ratification of the ACTA would not introduce any significant changes to the Polish copyright law order due to the fact that the level of enforcement in cases of copyright infringement provided for by the Polish law currently fulfils the requirements of the controversial Treaty.[17] This fact may seem incomprehensible given that the flagship argument of the anti-ACTA movement was that the Treaty would irreversibly change the face of Polish copyright law, and moreover, that as a result of the protests, government decided to organise a round-table negotiations that focused on the desirable shape of copyright law that would satisfy various parties to the dispute.

**18** This paradox might be better understood when one more general problem, highlighted both by the protesters and some public institutions supporting them, is considered. The opponents of the ACTA treaty raised the question of the role of copyright law in the information society, claiming that ratification of the ACTA treaty would lead to the petrification of the old copyright regime and preclude any potential attempts to modify it in the future.[18] They warned that such a situation endangers public interest, protection of which requires renegotiation of the social contract on which copyright protection is based. In their opinion, the new social contract should take into consideration social changes triggered by rapid technological development.

**19** This argument treated ACTA as the symbol of the very strong proprietary vision of copyright law as opposed to the more open model favoured by the protesters. The anti-ACTA movement might therefore be perceived as the act of objection towards a strong proprietary paradigm that is present in most current international regulations in the scope of intellectual property in general, and copyright law in particular.

## 3. Strong Proprietary paradigm vs Open Access approach. Conflict of norms

**20** In my opinion, such an approach that classifies the anti-ACTA movement as an example of the clash between the *strong proprietary* vision of copyright law present in the current intellectual property regime on one hand, and the *open access* paradigm on the other hand, is very promising and allows for treating these particular protests as an example of the wider social phenomenon present worldwide. I assume that the core of the current crisis of copyright law in the digital era can be found in the divergence between legal and social norms concerning the access to intellectual and artistic creations. I discern two main sources of the conflict between these two norms. The first is the result of the specific dynamics in the development of technology, copyright law and social norms, which are perceived as a global phenomenon. The second is the outcome of specific local particularities that led to the evolution of social norms, which differ considerably from the contemporary intellectual property regime. In both cases, however, the core of the problem lies in the fact that consumer held social norms (developed either on the global or local level) strongly oppose the *absolute property* rhetoric present in most of the international regulations in copyright law. The rejection of the *strong proprietary* vision of copyright law refers both to material and procedural elements of the current international intellectual property regime. This regime is characterised by the tendency to neglect needs of the end-users, and public interest in general, not only in the content of the legal regulations but also in the procedures applied in the legislation processes, which rely on the opinions of the copyright-holders, represented mainly by the powerful entertainment industries and collecting societies from primarily the developed countries whilst excluding the representatives of the civil society and the developing world.

# II. The anti-ACTA protests put in context

**21** In the Polish case both of the aforementioned sources of conflict between the legal and social norms intertwine. The first category is universal in its nature and explains resentment towards the strong *proprietary* vision of law both locally and globally; the second refers to the peculiar historical and social conditions in which specific Polish social norms regarding access to intellectual and artistic goods developed.[19]

**22** Due to the limits of this contribution, the second category, category of local conditions favouring development of social norms approving of *open access* to knowledge and culture and disapproving of the *strong proprietary* vision of culture, which is specific to Polish situation, will remain only signalised and not developed in detail. The more universal trends, stemming from the digital revolution and relevant for the developments in many parts of the world, will be analysed more closely.

**23** Therefore in the following section I will endeavour to explain why the anti-ACTA protests were not ignored by the government, but quite the opposite, were highly ranked on its political agenda and managed not only to change the governmental position with regard to the ACTA treaty, but also triggered further-reaching processes aimed at reforming Polish copyright law in accordance with emerging needs of the information society. In this analysis I will concentrate solely on the universal grounds that might have been relevant to the Polish situation and to that of the other states which experienced the anti-ACTA, or more general anti-strong-proprietary-copyright, movements.

## 1. Genesis of the conflict between the social norms and legal regulations. Technological revolution – contradictory expectations of the end-users and the copyright holders

**24** Before the digital revolution, as perceptively noticed by Ysolde Gendreau, *"copyright law was perceived, even by those in the legal profession, as an arcane and highly specialised area of the law. Its status as an intellectual property right that pertains to the arts helped to cultivate an aura of exclusivity around it. Few people studied it: few courses on it were offered in law schools. Today, the situation has changed radically."*[20] The situation changed after the introduction of digital technologies and the Internet. The new technologies affected both the legal regulations and the social norms held by the public. Technological revolution through computer facilitation made both artistic creation and access to the works of others available to everyone on an unprecedented mass scale. Due to the technological changes, but also due to the expansion of the content and creative industries, consumers became surrounded by copyrighted material. The contemporary world is bursting with music, film, photographs and other creative works and access to (and even distribution of) the works of others, as well as the possibility of creating one's own work based on the reuse and remix of existing materials, has become an inherent part of everyday life in the information society.[21] What was once only possibility turned into a need and a must. The sheer technological potentialities unknown before made the end-users change their attitude towards what should be legally allowed, and they led to an increasing number of postulates for unlimited access to knowledge and culture, based on the assumption that technological and legal possibilities should be equated.

**25** However, the same technological changes that led end-users to articulate their postulates for freedom of information and culture were used by the copyright holders to reinforce the legal protection of their rights. End-users who expected more access were faced with increased protection of works with the proliferation of "secondary" remedies,[22] such as the technical measures blocking the copyrighted material even against the legitimate acts of consumers and the introduction of legal regulations protecting these technical measures against circumvention.[23]

**26** This protection of copyright holders' commercial interests has been perceived by the consumers as being introduced at the expense of the public needs and led to the initial problems with the image of copyright law. This reinforcement of copyrights not only went against the new expectations that emerged with the novel technologies, that allowed for the cumulative research and creativity on a scale unknown so far, but also went against the entrenched social norms that favoured a private use exception,[24] which was seriously weakened by the new technological and legal shields used by the copyright holders.

**27** Also, exactly at this point, the place of copyright law in the public discourse drastically changed. Nowadays copyright law is one of the mostly discussed legal issues present in the public debate around the world, often taken up by laymen. *"This heightened visibility* – [however, as Gendreau emphasises] – *has not translated itself into a greater degree of popularity. On the contrary, copyright law has an image problem."*[25]

**28** In the following sections I will endeavour to explain both why an image of law and law understood as the normative reality is important for the discussion on the relation between the legal and social norms, and what the causes are of the observed unpopularity of copyright law among the general public.

## 2. The image of law and its influence on social norms

**29** The general public, as opposed to lawyers, usually has no specific professional knowledge in the field of law, and thus its attitude towards legal regulations depends not solely on the particular norms and its influence on the social reality, but also on the image of those regulations. Whether the society respects given law and obeys particular legal norms depends not only on the normative reality, but also on the way in which the society *perceives* the particular branch of law. What the general public thinks the law says and how it apprehends respective legal acts is equally important for the internalisation of the legal norms as what the law actually says. The importance of the image of law originates in the fact that both legal and social norms, as well as the process of their internalisation, are social facts. The notion of *'social fact'* is used here as understood by Emile Durkheim,

i.e. as an independent entity that has its origins in the respective society, owes its characteristics to the specificity of that society, and would not have existed if not for that society.[26] Already at the dawn of sociology, Durkheim and Weber asserted that social facts construct the social reality that is separate and autonomous from the material world and, as such, is ruled by distinct principles.[27] Social reality is created not only from *what is* but also equally from *how people perceive what is*. Thus, according to Weber, the appropriate cognitive category for the analysis of the social reality ought to be inter-subjectivism, as opposed to objectivism, which should be reserved for the analysis of the material world solely.[28]

**30** Basing on the aforementioned theoretical assumptions, this chapter is also guided by the hypothesis that as the internalisation of legal norms is a social fact - an element of the social reality that does not belong to the material world - its analysis should use inter-subjectivism as a cognitive tool. That is why in the analysis of the mutual interaction between the legal and social norms, not only should the so-called *objective*[29] normative plane be taken into consideration, but also the intersubjective dimension of the copyright law – its *image*, i.e. the way this branch of law is perceived amongst the general public. This expansion of the scope of research from *what the law is* to *what society thinks the law is* allows for the conclusion that the negative representation of copyright law is yet one more reason, besides the technological revolution, for the emergence of social norms that diverge significantly from the current copyright regime.

## 3. Why copyright law suffers from an image problem

**31** This section will refer to the concept of *image of* law, understood as an inter-subjective perception of what copyright law is. It will describe the popular image of contemporary copyright law, based on the presumption that the general public, as a rule, perceives copyright law in the negative light and that this negative perception impedes obedience to its norms. Furthermore, this section will aim to explain the manifold reasons for this observed image problem.

**32** One of the most important causes of copyright's bad publicity is the perceived disappearance of the creative author from the system, who has instead been replaced by the huge companies that possess and manage the copyrights in millions of works of art produced by the thousands of creators,[30] and by the collecting societies that are equally anonymous and far from the source of the creative process.[31] Consequently, profit for the distributors of the creative works has lost its public acceptance and the copyright norms assuring this profit have been perceived as illegitimate because the marginal cost of the reproduction and the distribution of most of the works in the digital era have become minimal.

**33** A following reason for the bad image of copyright law is the current trend of strengthening protection, together with the globalisation of more general intellectual property standards, which in many countries is perceived as American *neocolonialism*[32] due to the fact that it imposes a vision of copyright that originates in the U.S. and does not necessarily correspond to other legal traditions; not to mention the role of the American entertainment industry in the drafting of the current international copyright regime. The notorious cases of Pirate Bay, Richard O'Dwyer and others reinforce this vision of copyright as the tool for the worldwide expansion of American corporations due to the doubtful legality of the application of American law outside U.S. territory.[33]

**34** This negative picture emerges also as a result of the extreme opaqueness of the negotiation and legislative process of recent international treaties regulating intellectual property issues, best exemplified by the ACTA case. The negotiations of the Anti-Counterfeiting Trade Agreement were secret and the first bits of information about the proceedings leaked through WikiLeaks in May 2008, followed by the numerous press reports and scientific articles. Leading non-governmental organisations advocating for the digital citizen's rights from all over the world urged for more transparency in the negotiation proceedings and more inclusiveness,[34] as the initial documents were drafted without the participation of civil society groups and representatives of the developing countries. They also referred to the negative influence of the negotiations' secrecy on the general public's perception of the drafted document.[35] Nevertheless, the call to open up the negotiations was ignored; instead the negotiating parties justified secrecy by the nature of the negotiated interests.[36] Still, secrecy of the negotiations was perceived negatively by the citizens' organisations that treated the lack of transparency as proof of the negotiators' bad intentions. Their concerns were shared by the European Parliament, who urged for transparency and called on the European Commission to *"immediately make all documents related to the ongoing international negotiations on the Anti-Counterfeiting Trade Agreement (ACTA) publicly available"* in its resolution of 10 March 2010.[37] The adamant position on the secrecy of the negotiations taken by the involved parties, which remained long unchanged notwithstanding the pressure of the various groups urging for transparency and inclusiveness, shaped a very negative image of the ACTA document still at the drafting level and that played an essential role further on in the protests against its ratification.

**35** The atmosphere of opaqueness, conspiracy and hatching perceived by the general public as aimed against its interests is present not only in the negotiation process of international treaties, but also in the case of domestic agreements that point at enforcing copyright law.[38] Copyright holders explain the need for secrecy by the professional character of trade consultations, which should involve only the commercial players and exclude the general public. This approach originates in the period before the technological revolution, when indeed copyright law was the arcane arena of authors and only a handful of specialised lawyers. However, with the introduction of the Internet and digital technologies, the situation has drastically changed not only because of the shift in the consumers' attitudes. The new technologies have changed social reality by providing general public with so far unknown means of expression; hence what before amounted to regulations concerning only a small number of professionals now refers to everyday practices of the general public. Moreover, the unbalanced protection of copyright interests on such an unprecedented scale endangers some fundamental rights such as privacy and freedom of expression. Therefore what used to be a highly specialised domain of law, where only professionals could negotiate amongst each other, now needs the inclusion of the general public.

**36** Nevertheless, the inclination to conceal originates also in the presumption that protection of copyright holders necessarily involves fight with the end-users. The copyright campaign is, in fact, called a *copyright war* - a war between the end-users on one side and the intermediaries in the market for the intellectual goods on the other. The secrecy of the negotiations is just one of the examples of belligerent strategies: you do not negotiate with the enemy. Another involves the application of criminal law and linguistic battles that shape the discourse of copyright law.

**37** Excessive criminalisation of acts that go against the norm of protecting creative works, which shifts the burden within the branch of copyright law from the civil to the criminal regulation, is one more reason for the bad image of copyright law.[39] This belligerent strategy was first invented in the mid-90s of the last century in the U.S. with the expansion of the digital technologies that empowered consumers in an unprecedented way.[40] It was initially epitomised by the strengthening of criminal penalties for copyright infringement and was soon followed by the aggressive litigation campaigns aimed not only against the commercial entities but also against ordinary citizens. Finally, the last step added to the already destroyed image of copyright law was both the dangerously rising number of litigations against consumers, and the biased method of ascertaining the responsible person based mostly on IP addresses, leading to ridiculous outcomes of teenagers, or even the deceased, being sued.[41] These litigations, in which individuals were obliged to pay unreasonably high damages to the copyright holders for illegal *file-sharing*, completely destroyed the already poor perception of copyright law for the general public.[42]

**38** Started in the U.S., the copyright war with the consumers has spread all over the world. The best instantiation of this strategy in Europe is the French *HADOPI* law,[43] which introduced a so-called *three strikes* policy that is aimed at encouraging compliance with copyright law in the digital environment, and which allows for internet access to be blocked for the holder of the IP address from which the copyright infringement has supposedly been committed. The British *Digital Economy Act* is just another instantiation of this process.

**39** The American and French examples of regulations aimed at fighting copyright infringement in the digital environment through criminal proceedings against the end-users show that this strategy is very harmful in terms of image, as consumers have started to perceive copyright law mostly as an unpredictable weapon pointed against them, and so their respect towards this branch of law has greatly diminished.

**40** The tendency to aim criminal sanctions against the private persons who infringe copyright through private use, and not in commercial dealings, has also marked an important shift within the copyright regime as these means had so far been reserved for the unfair competitor, who copied and distributed copyrighted material for profit without the proper authorisation. The same shift can also be observed in the linguistic plane as copyright holders, mostly intermediaries, have come to describe copyright infringements committed by the end-users as *piracy* – a notion that was again so far reserved for the commercial entities.[44] These two tendencies have also really harmed the popular image of copyright law because they have blurred the borders between the infringing acts of consumers and the *real piracy*, i.e. large-scale copying and sale to the public by for–profit actors.[45] This confusion of the terms and actions leads to the trivialisation of *piracy* in the perception of the general public as it sees no difference between arresting teenagers, deceased, the innocent or just those who commit a copyright infringement in non-for-profit dealings, and the criminal proceedings against the entities that base their commercial activity on the non-authorised mass reproduction and distribution of the copyrighted material. In such a situation myths of the martyrs sacrificing themselves for the supposed sake of freedom of knowledge, culture and the Internet, are easily created and lead to an increasing decline in respect for copyright norms. Moreover the application of the belligerent strategies that have been used thus far by the copyright holders to stop the acts of unfair competitors profiting from the unauthorised distribution of copyrighted materials

seem to be completely inadequate with regards to the end-users, as they, contrary to the competitors, are actually the target group of the creative and content industries, and their cooperation is essential for the provision of profit to the copyright holders. The *copyright wars*, instead of convincing consumers to respect copyright law and contribute financially for the access to intellectual and artistic goods, only encouraged consumers to apply various strategies to oppose the current regime, which will be described in detail in the next section.

**41** Further cause for the negative image of the copyright law is the further prolongation of the terms of copyright protection that, for an average individual, seem nearly eternal. This adds up to another problem concerning the terms of protection – they seem arbitrary due to the fact that the optimal duration of copyright protection has never been assigned and proven scientifically.

**42** The above described multiple factors result in the very negative image of the current copyright regime that is shared by the growing number of end-users as the role of the copyright regulations in the information society have become an important topic in the public debate around the globe. This negative image, added to the new expectations of the end-users that arose with the technological revolution, led to the discrepancy between the legal regulations and the social norms[46] held by the public with regards to access to knowledge and culture. This discrepancy subsequently resulted in additional costs of compliance with the law. The following section will be devoted to the description of the various reactions of the end-users faced with the tension between *what they perceive as fair* in terms of copyright protection and *what the law allows for*, which led to the situation where obeying the law became onerous.

## 4. The response of the environment – end-users' reaction to the discrepancy of social and legal norms

**43** Current legal scholarship abounds with works developing various options available to regulators, ignoring, however, the reaction of the regulated to the given laws.[47] Copyright law is no different, if not a perfect example of such an approach, which stems from the positivist thinking of law as a separate entity, independent from other social processes. Nonetheless, this paper, as already mentioned, is based on the assumption that an in-depth analysis of the current crisis of copyright law requires the reaction of the regulated to be included in the research model.

**44** There are various types of the regulated groups and even though they might be regulated by the same piece of legislation stemming from the same regulator, the law will still concern them in different ways. Needless to say, in the case of copyright law, the same regulation has various effects on copyright holders and the end-users. Therefore, their attitude towards law differs and so does their reaction towards respective pieces of legislation. The model therefore has to take into consideration the various interest groups among the regulated.

**45** Hence, this section will analyse what the impact of copyright law is on both interest groups, and it will show what strategies are available to them when dissatisfied with the regulation. The model considers both the copyright holders and the end-users. However, given that the main topic of this analysis is the current trouble with compliance in the domain of copyright law, more focus will be put on the reaction of the end-users to the expansion of the copyright regime. The chapter is based on the assumption that the bad image of copyright law and the conflict between the legal regulations and the norms held by the general public with regards to the distribution of, and access to, the copyrighted goods, has led to additional costs of compliance with the copyright law and will analyse various strategies that end-users apply to try to lower those costs, showing also how they differ from the strategies available to the copyright holders[48].

**46** The theoretical introduction will be followed by practical examples, showing how the interaction between the regulator, the law and the regulated shapes the current situation in the field of copyright law in the digital era.

**47** There are two main bodies of scholarship that describe the options available for the regulated when faced with burdensome law.[49] The compliance literature suggests that groups try to *avoid* laws that they find too costly to comply with, while the political choice literature on the other hand suggests that groups in such situations tend to *change* the law. Both bodies of scholarship analyse various cases in which law may become burdensome. In this model, the conflict of social norms held by the end-users with the legal norms will be treated as the main reason for the high costs of compliance. Subsequently, the concept of *political salience* will be introduced as another dimension influencing the dynamics between the *strategies of avoidance* and *change*.

### a. The Model of Compliance and the Strategy of Avoidance

**48** In its simplified version, the model of compliance might be presented as a statement according to

which, *"Laws are followed when the expected costs of legal punishment exceed the expected benefits of the banned behaviour."*[50] There are, however, two sets of external factors that contribute essentially to the compliance of law: 1) social norms and 2) investment in mechanisms that allow avoidance of sanctions.[51] These two sets of factors that influence compliance with the law are interdependent and as such should be taken into consideration simultaneously. Hence the conflict of social norms with legal regulations may lead to initial disinclination to comply,[52] which is further developed if mechanisms to avoid sanctions are available. In other words if social norms are not in line with the legal regulations, groups may seek to avoid complying with the law while at the same time trying to avoid sanctions. The reverse situation is also plausible when the availability of mechanisms allowing for the avoidance of sanctions, i.e. lack of effective enforcement of law, leads to changes in social norms and as a result lowers the level of compliance. In the critical situation of a very serious clash between the social and legal norms, the regulated shun compliance and stop avoiding sanctions; quite to the opposite, they want to be punished to prove the injustice of law. This is how civil disobedience or revolutionary movements are born.

**49** According to the compliance literature, mechanisms allowing for the avoidance of problematic legal regulations may take two forms: *evasion*, understood as an investment in trying to decrease the odds of being punished for violating a law[53] or *avoision*, which can be defined as efforts to exploit the differences between the law's goals and its self-defined limits.[54] End-users' strategies of file-sharing, leading to the avoidance of copyright regulations in fact take both forms: the former being best exemplified by the application of various types of software enabling anonymity in the networks, and the latter instantiated by the sharing platforms that create an illusion that the *file-sharers* are indeed close friends, which would allow them to rely on private copying exception.

**50** Both types of *avoidance strategies* involve individual action, where no cooperation between the subjects of the law dissatisfied with its functioning is required. Thus the *avoidance strategy* is perfectly suited for unorganised large groups of end-users. This is not the case when it comes to the *strategy of change*, as the following section should suggest.

### b. The Model of Political Choice and the Strategy of Change

**51** The literature on political choice has distinguished between two major types of strategies that change the law that the regulated find burdensome: *litigation* and *lobbying*. The former strategy is probably more effective in the common-law systems, where the law is modified on the basis of the cases decided by judges, and it is best exemplified by strategic litigations. Both instantiations of the *strategy of change*, however, differ from the *avoidance strategy* in that they require a collective action on the part of the dissatisfied regulated groups in order to be effective in modifying the legal regulations. Therefore small, well-organised interest groups are much more effective in changing the law than large, unorganised groups. Hence when the benefits of law are concentrated and its costs are diffuse, a small well-focused interest group will usually succeed in obtaining passage of a law, even if it does not benefit society as a whole.[55]

**52** In compliance with these theoretical assumptions is the case of copyright law where the *strategy of change* had so far been reserved to the right holders, represented mainly by the intermediaries in the market for knowledge and artistic goods or collecting societies. The general public, as a large unorganised group, rather had to resort to the above described *strategies of avoidance*, for *the strategy of change* was too burdensome because it involved collective action problems, which were difficult to overcome by large or loose groups. Therefore, the sheer nature of the *strategy of change* renders it much more easily available for the well-organised interest groups than for the general public, which resorts to the *avoidance strategies* (See the table below).

Strategies of avoidance vs Strategies of change

| STRATEGIES OF AVOIDANCE | STRATEGIES OF CHANGE |
|---|---|
| No collective action needed | High cost of collective action |
| Perfectly suited for large, unorganised groups | Suited for small, well-organised interest groups |
| Used so far by the end-users unsatisfied with copyright law | Reserved so far for the copyright holders |

**53** The following section will introduce another dimension to the model in which the mutual interactions between the regulator, the regulated and the law are analysed – the importance of *political salience* of the regulated domain. It will show that *political salience* is yet another factor that advantages the well-organised interest groups in influencing law over the general public.

### c. Political Salience and its influence on the Strategies of Change

**54** The political scientists use a concept of *political salience*, understood as the importance of a political issue to an average voter relative to other issues.[56] Issues of *high political salience* are the issues that are important for the general public, topics on which the

public discussions focus and which serve as the basis for formulating electoral programmes. Nevertheless, many issues in capitalist democracies are not subject to a general vote[57] either because the nature of those issues is too complicated for the general public to formulate opinions on, or because the *median voter* perceives them as irrelevant.[58] Issues of *high political salience* win elections; those of *low political salience* have no significant influence in the political race between the parties. Issues of *low political salience* are absent in the mainstream media; hence, they create no incentives for politicians to gain expertise in them. Nonetheless, even though the *issues of low political* salience do not formulate a part of the public political discussions, they might be of crucial importance for some organised interest groups. The lack of public interest, and consequently, the lack of media coverage and in-depth knowledge of the issue among the politicians, *"create an ideal political terrain for interest groups with a concentrated interest in the outcome of the political process."*[59] These groups do not need to resort to the elections as the method of realising their interests. In most cases, they apply *quiet politics*[60] in which they use soft methods of convincing politicians into protecting their interests during the meetings and negotiations that remain invisible to the general public. Consequently, as a result of negligence, decision-makers often lack competence in challenging the expertise of the interest groups and do not posses counterbalancing arguments that could have been developed by the general public, and hence remain prone to the persuasion of strong business powers.[61]

**55** The situation changes however, once the general public starts paying attention to a particular issue, turning it from a matter of *low political salience* into a one of *high political salience*. The interest of the general public is interdependent on the mass media coverage and both of these factors increase the interest of the decision-makers in the issue. Thus if the voters care about an issue, the politicians will start paying attention, trying to win the public support. However, for the public opinion to be strong enough to counterbalance the power of concentrated interest groups, the voters need to retain their interest in the issue. *Temporary political salience* will not suffice to incentivize journalists and politicians to develop an expertise in the issue, especially when the issue is complicated.[62]

**56** Therefore, as it may be inferred from the above argumentation, the *low political salience* of a particular issue becomes equivalent to the nature and impact of the *strategy of change*, giving the advantage to the well-organised interest groups over the general public. The history of the development of copyright law proves once again the general theories developed by the political scientists. Hence, not only does it confirm the relevance of the *strategy of avoidance* vs. *strategy of change* dynamics, but also the importance of the *political salience* dimension in favouring copyright holders against the end-users.[63]

### d. Power shift?

**57** According to the above presented argumentation, the *low salience* of copyright law, which until recently has been absent in the public discourse, constituting instead a domain reserved for the right holders and specialised lawyers, as well as the difficulty with applying the *strategy of change* by dissatisfied with the law end-users gave the general public no significant influence on the regulation in the domain of access to knowledge and culture.

**58** Nevertheless, the digital revolution situation has changed the scene drastically. Firstly, the fact that today, anyone can be subject to copyright regulations, either as a creator or as an end-user getting access to or distributing the works of others, turns the copyright regulations into an issue of *high political salience.*

**59** Secondly, thanks to Internet communication, especially social networking and online petition services, the difficulties associated with supplying public good in the form of a modification of the existing law are surmountable, and thus the strategy of change becomes available to the general public. As is very well exemplified by the phenomenon of the Pirate Parties and the influence of the recent anti-ACTA protests in Europe, the digital revolution has facilitated the birth of a new lobbying power in the copyright regulation domain – the power of the end-users.

**60** The *political salience* of an issue differs between societies and might be conditioned by specific historical experience. Hence *political salience* of copyright law differs between the countries and recent events prove that it is in fact much higher in Poland[64] than in the Western states, which is what motivates Poles more than Western societies to resort to the *strategies of change* of an onerous law, which could help in attaining a compromise between the conflicting interests in the digital environment.

## 5. The anti-ACTA movement as a strategy of change of the onerous law

**61** As the above described analysis suggests, the Polish anti-ACTA movement and its influence on the governmental strategy on the scope of copyright law in the digital environment could be explained by the application of the model based on the concepts of *strategy of change* of the onerous law and *political salience* of the copyright law.

**62** Interestingly enough the Polish government understood the *high political salience* of the *ACTA conflict* and reacted to the social dissent by applying a well-proven method used in Poland in the transition period: the round table negotiation.

**63** The Polish case may set a positive example for other European States challenged by the rapidly changing needs of the digital environment. Nevertheless, the power of social norms will only be able to change the law if the general public does not lose its interest in the case, especially since the new strategy of the government concerning intellectual property law does not legally bind its successors. Therefore, *temporary political salience* will not be enough, and will once again only lead dissatisfied end-users to avoid burdensome regulation and consequently, to develop profound disrespect for copyright law.

## B. Conclusion: The anti-ACTA movement as a lesson of participatory democracy. On the importance of procedural justice.

**64** As the above provided analysis proves, the crucial reason for disregard towards regulations of copyright law and resistance towards the current international intellectual property regime lies in the negative image of the copyright law and its influence on social norms. Both the personal statements of the anti-ACTA movement participants in Poland quoted at the beginning of this paper and the further analysis of causes for the negative image of copyright law worldwide indicate that elements of the *material* and *procedural* nature are equally important to the public in the process of perception and evaluation of the given branch of law.

**65** This observation is in line with findings of the research in the scope of social sciences, which proves that individuals value *procedural justice* as much as *material justice*, and that in some cases adequate application of rules of *procedural justice* may improve perceptions of *material* law.

**66** *Material justice* is here understood as being represented by two types of justice: *distributive justice*, which means *"fairness in the distribution of rights or resources"* and *restorative justice*, which refers to *"fairness in the punishment of wrongs." Procedural justice* on the other hand refers to the *"idea of fairness in the processes that resolves disputes and allocates resources."* The concept of *procedural justice* includes *"neutrality, lack of bias, honesty, efforts to be fair, politeness, and respect for citizens' rights."*[65] Essential is also a concept of *inclusiveness*, which allows all parties to the dispute to participate in the decision-making process.

**67** The concept of different types of justice is not a new one; nevertheless, assurance of the proper realisation of the rules of procedural justice is still problematic in many democracies, which theoretically should be based on the idea of the rule of law. Copyright law is the best example of this problem.

**68** It is worth emphasising that the decision of the Polish government to launch negotiations on the round table open to all parties interested in the problems of copyright law in the digital era; the rules of transparency that governed the consultations; as well as the outcomes of the negotiations are all manifestations of the proper application of rules of *procedural justice*. Given the fact that material norms of copyright law are not that easily changed because many provisions stem from international regulations, legislators should concentrate at least on implementing the rules of *procedural justice,* which might considerably improve the image of copyright law and as a result lead to an increase in respect towards its rules. The safeguards of *procedural justice* should become a priority in copyright policies, especially since social scientists prove that an individual's identification with decisions increases when he or she is involved in the process assuring procedural justice. *"Where people feel that they have control over decisions they believe that the procedure is fair; where they feel they lack control they believe it is unfair."*[66] Moreover *"depending on the procedural justice processes of the group, the social identity of the members will be influenced accordingly and different values will be emphasised. The more a member agrees with the type of procedural justice employed, the more they will identify with their group. This increased identification results in the internalisation of the group's values and attitudes for the group member. This creates a circular relationship as the group's procedural justice processes will affect group members' levels of identification and, as a consequence, this level and type of identification will affect their own values of what is fair and unfair."*[67] The influence of *procedural justice* on identification with norms regulated by law should be perceived as the more important given the current conflict of legal regulations with social norms, which leads to the situation in which the general public usually treats copyright law as *unfair*.

**69** It is worth reminding that the slippery slope on which the positive (or neutral) image of copyright law was gradually sliding down was first introduced in the U.S. already in the *"first decade of the twentieth century, when Congress faced the problem of updating and revising a law that was perceived as too arcane and complex for legislators to understand without expert assistance. To solve that problem, members of Congress prodded the Librarian of Congress to set up a series of meetings with representatives of industries with an interest in copyright"*[68]. Since then, legislative processes in many countries have involved the excessive influence of the representatives of the

right holders with the exclusion of the end-users. Recent social and technological changes prove, however, that the time is ripe for changes that would introduce *procedural justice* with regards to the access to legislative processes, before any material changes improving the situation of the end-users might be introduced.

**70** Representatives of WIPO have in the recent past repeatedly stated that the multi-stakeholder environment is *"the best and most appropriate when it comes to the debate on copyright in the digital age, (and that) WIPO is preparing for such multi-stakeholder discussions."*[69]

**71** The European Commissioner responsible for the Digital Agenda in Europe also promoted the method of round table negotiations on many occasions. Neelie Kroes, who claimed that open public dialogue is the only way to achieve a long-standing compromise between the conflicting interests of various stakeholders in the digital environment, said this would assure compliance with copyright law. A similar approach has also been taken by Michel Barnier, the Commissioner responsible for Internal Market and Services. So far, however, most of the decisions in the European Union in the scope of copyright law have been taken in accordance with the logic of *quiet politics*, where low salience of the issue and the difficulty in changing the law by the unorganised general public, favours lobbying of the small but strong interest groups.

**72** In these circumstances, the new *post-ACTA* approach of the Polish government towards copyright policy might set a positive example in the international arena, showing how procedures of the *round table* applied in the transition period, enhanced by the new communication technologies, might be useful in building participatory democracy and solving contemporary problems that are common for all of the European states.

■

* The paper was presented at the "1st International Research Forum on Law and ICT/IP" on7th / 8th of November 2012 at Georg-August-Universität in Göttingen, Germany. The Colloquium is an annual event and provides the opportunity for young researchers to present the results of their scientific work and obtain valuable feedback from senior academics and practitioners in the field of ICT and IP Law.

I would like to express my gratitude to Prof. Giovanni Sartor, supervisor of my doctoral thesis "Copyright in decline? Systems theory, autopoiesis of law and the crisis of copyright law in digital era", as well as to Dr. Julia Hörnle, who not only gave me a very detailed feedback that allowed me to improve my work, but also inspired and encouraged me for further research.

1 Hereinafter referred to as the ACTA treaty, ACTA agreement, controversial treaty or the Treaty.

2 The proceedings of all the consultations are available online (in Polish) at: http://warsztaty.mac.gov.pl/ [Accessed on 31.01.2013].

3 Just before the anti-ACTA movement was born in Poland, the Polish government had been faced with smaller demonstrations concerning GMOs and reform of the national health system, in which the ruling coalition did not involve wide social consultations, trying instead to ignore the public discontent and carry on its own projects at all costs. The government was repeatedly criticised by the media and representatives of the civil society for not paying due attention to the public opinion and attempting to rule with an iron fist. At the beginning of the anti-ACTA protests, when the government had not yet managed to assess adequately the scale of discontent, it tried to apply its old methods by ignoring the protesters and ridiculing the whole movement. It was only in the later stage, when faced with the massiveness, long duration and wide territorial scope of protests, the government decided to change its strategy and initiate a serious dialogue with the protesters. *See:* Żakowski, J.,"Porozmawiajcie z nami," *Gazeta Wyborcza,* 30.01.2012.

4 One of the first steps taken by the Polish government with this new post-ACTA approach, not directly connected with the copyright issues, was the decision not to sign the International Telecommunications Regulations in Dubai in December 2012 without first engaging in profound social consultations. Notwithstanding the initial consultations before the World Conference on International Telecommunications, the Ministry for Administration and Digitization decided to open a wide public debate on the ITRs that would be accessible online, giving every interested individual an opportunity to comment on or criticise the Regulations and to show one's opinion on the potential accession of Poland. *See:* http://mac.gov.pl/wiadomosci/rozpoczynamy-konsultacje-miedzynarodowych-regulacji-telekomunikacyjnych-itr-w-wersji-przyjetej-w-dubaju-ale-nie-przez-polske/ [Accessed on 31.01.2013].

5 The protests that started in Poland in January spread to many European countries in February. On the 4th of February 2012, hackers who identified themselves as belonging to Anonymous and CyberForce groups blocked the websites of the Swedish government on the same day the protests began in the streets of Sweden. *See*: PAP (Polish Press Agency), "Anonymous przeciwko ACTA w Szwecji." *Rzeczpospolita*, 04.02.2012. On the 11th of February 2012, a pan-European protest inspired by the Polish demonstrators took place in many European cities including Munich, Salzburg, Vienna, Graz, Praha,Tallin, Vilnus, Riga, Sofia, Budapest, Paris and Bucharest. See: PAP (Polish Press Agency), "Przeciw ACTA. Dzień demonstracji w Europie." Gazeta Wyborcza,11.02.2012.

6 The European Commission confirmed on 20 December 2012 that it was withdrawing ACTA referral to the Court of Justice of the European Union, which confirms the rejection of the Treaty by the European Union at this point.

7 Grynkiewicz, T. "ACTA podpisana, temperatura nie opada." *Gazeta Wyborcza,* 26.01.2012; PAP (Polish Press Agency), "ACTA. Demonstracje w kraju." *Gazeta Wyborcza*, 11.02.2012.

8 Ibidem.

9 The phenomenon of the anti-ACTA movement in Poland is being analysed by many research groups; however it seems that the most extensive and coherent research has been conducted by Zespół Analiz Ruchów Społecznych (Team for the Analysis of Social Movements) see: http://zars.home.pl/autoinstalator/wordpress/zars/. The results of their sociological intervention and quantitative research, as those of the other research groups, has not been published so far. Therefore the description of the anti-ACTA movement in Poland presented in this contribution is based solely on the analysis of the discourse shaped by the representatives of various interest groups present in the media. Publication

of the results of the qualitative interviews and quantitative research may consequently enrich my reasoning in the future.

10 *See*, e.g.: Danielewski, M., "Acta jak wystrzał z >>Aurory<<," *Gazeta Wyborcza,* 26.01.2012.

11 *See:* ante, footnote number 9.

12 This categorization of the reasons for objecting the ACTA treaty into *material* and *procedural* intentionally plays with the conception of *procedural* vs. *material* justice that will be applied in the paper later.

13 Article 9 of ACTA reads as follows: "In determining the amount of damages for infringement of intellectual property rights, a Party's judicial authorities shall have the authority to consider, inter alia, *any legitimate measure of value* the right holder submits, which may include lost profits, the value of the infringed goods or services measured by the market price, or the suggested retail price" [emphasis added]. Polish copyright law regulates question of damages in case of copyright infringement in Article 79. 1 b) of the Polish Copyright Act, which refers to the doubling of damages, and in cases when the infringer is culpable – triple the amount of the royalties that the end-user would have had to pay to get legal access to copyrighted work.

14 Judgement of 16.09.2011 in the case *Sony BMG Music Entertainment* against Joel Tenenbaum, in which the court obliged a minor to pay damages in the amount of $675,000 for the infringement of copyright through illegal *file-sharing*, is a good example of the threats to which protesters were referring. *See:* Judgement of 16.09.2011 *Sony BMG Music Entertainment vs. Joel Tenenbaum,* United States Court of Appeals for the First Circuit, Nos. 10-1883-10-1947, 10-2052. Available at: http://www.ca1.uscourts.gov/pdf.opinions/10-1883P-01A.pdf.

15 *See:* Wiewiórkowski, W. *Opinion of the General Inspector for the Protection of Personal Data of 23 January 2013*; Lipowicz, I., Opinion of the Ombudsman of 25 January 2013.

16 The Ombudsman also quoted the Constitutional Tribunal which stated that:

*"[T]he principle of citizens' trust in the state and its laws is based on the legal certainty (...) which ensures legal safety to each individual. This enables each individual to decide on their behaviour based on the full knowledge of the premises of the state authorities and the legal implications of what her actions may entail. Every individual should be able to determine the consequences of specific behaviours and events on the basis of the law currently in force as well as to expect that the law will not be changed arbitrarily. Legal safety of each individual, therefore, allows for predictability on the part of the state authorities (...)"*

The Ombudsman stated that the government did not apply the principle of legal certainty during the negotiation and ratification of ACTA, and thus acted against the constitutional rule of law.

*See:* Lipowicz, I., Ibidem, p. 2; Article 2 of the Constitution of the Republic of Poland reads as follows: *The Republic of Poland shall be a democratic state ruled by law and implementing the principles of social justice.*

17 *See e.g.:* Interview with Prof. Jan Błeszyński in: Wielowieyska, D. "Prawo autorskie znacznie surowsze niż ACTA," *Gazeta Wyborcza*, 27.01.2012.

18 This argument was also raised by the Ombudsman, *See:* Lipowicz, I., Ibidem, p. 3; *see also:* Interview with Katarzyna Szymielewicz, President of Panoptykon, important Polish NGO engaged in the protection of fundamental rights in the information society, leading institutional actor in the anti-ACTA protests in Poland in: Płociński, M., "ACTA czyli z armaty do komara" Rzeczpospolita, 20.01.2012. For more information on the Panoptykon organisation (also in English) see: http://www.panoptykon.org/node/112.

19 I develop this argument further in my PhD thesis *Copyright in decline? Systems theory, autopoiesis of law and the crisis of copyright law in digital era*, which I am currently finalising under the supervision of Prof. Giovanni Sartor at the Department of Law of the European University Institute in Florence. Part of the analysis present in my PhD thesis is strongly inspired by the Evolutionary Institutional Theory, which holds that contrary to the omnipresent trend of globalising legal regulations, social norms that guide human behaviour with regards to law develop gradually in response to local social, economic, and historical conditions. As a result, I argue that the peculiar historical conditioning of Polish society, from the partition of the country in the 18th century to the experience of communist regime in the 20th century, characterised by a strong censorship regime impeding the access to knowledge and culture and normal circulation of various intellectual creations, favoured development of social norms approving of informal and illegal circulation of copyrighted works long before the digital revolution. For the more detailed historical analysis *see* also: Gracz, K., "Bridging the gaps between the social and legal norms concerning protection of intellectual and artistic creations: on the crisis of copyright law in the digital era." *The Journal of World Intellectual Property*, Blackwell Publishing Ltd, (forthcoming 2013). Draft available at: http://www.atrip.org/Essays [Accessed on 31.01.2013].

20 Gendreau, Y., 'The Image of Copyright,' E.I.P.R., 2006, 28 (4), 209–212, p. 209.

21 The increasing popularity of social media partially stems from the fact that they are based on the concept of posting and re-posting copyrightable works of various genres: music, photographs, articles.

22 Gendreau, Y., *op. cit.* p. 210.

23 Requirement for anti-circumvention laws was globalised in 1996 with the creation of the WIPO Copyright Treaty.

24 At least in countries with continental law that introduce *private personal use* clause. The British copyright system, for instance, does not introduce the institution of the *private copy* so the expectations of the British end-users might considerably differ from their counterparts in continental Europe. On the other hand, however, the *Hargreaves Report* recommended the introduction of a private copying exception for the Internet, partly because of social norms demanding it. The report is available at: *www.ipo.gov.uk/ipreview-finalreport.pdf.*

25 Gendreau, Y., *op. cit.* p. 210.

26 Durkheim, E. *"Socjologia i jej dziedzina badań,"* tłum. Szacki J., Trybusiewicz J., *in: Filozofia i socjologia XX* wieku, part 1, Warszawa 1965, p. 118.

27 Ibidem.

28 *See:* Szacki, J., *Socjologia rozumiejąca Maxa Webera* in: *Szacki, J., Historia myśli socjologicznej.* Wydanie nowe, Wydawnictwo Naukowe PWN, Warszawa 2003, pp. 458-495.

29 Whether the normative reality might be treated as objective is also doubtful as it emerges in the process of constant interpretation and as such should also be treated as an inter-subjective social fact, which seems obvious for sociologists but not always for lawyers.

30 *See*: Ginsburg, J.C. "How Copyright Got a Bad Name for Itself" *26 Colum. J.L. & Arts 61 (Fall 2002)*, pp.61-62.

31 Gendreau, Y., *op. cit.* p. 210.

32 E.g. One of the major accusations raised by the opponents of the ACTA was the fact that the treaty was instantiating a vision of copyright law developed by the U.S. that would be imposed on other signatories. Similar arguments had been earlier raised with regards to the ratification of the TRIPs.

33 *See e.g.:* Halliday, J. *Richard O'Dwyer: leaked memo exposes lobbying by Hollywood studios*, The Guardian, 08.08.2012,

available at: http://www.guardian.co.uk/technology/2012/aug/08/richard-odwyer-leaked-memo-hollywood-lobbying [Accessed on 31.01.2013]. *Pirate Bay Founder Arrest Followed by &59m Swedish Aid Package for Cambodia* at: http://torrentfreak.com/pirate-bay-founder-arrest-followed-by-59m-swedish-aid-package-for-cambodia-120905/ [Accessed on 31.01.2013].

**34** In the open letter signed by numerous citizens groups and consumers associations such as Consumers Union, Electronic Frontier Foundation, Essential Action, IP Justice, Knowledge Ecology International, Public Knowledge, Global Trade Watch, U.S. Public Interest Research Group, IP Left (Korea), Australian Digital Alliance, The Canadian Library Association, Consumers Union of Japan, National Consumer Council (UK) and Doctors without Borders' Campaign for Essential Medicines, the representatives of the advocacy groups wrote: *"We are writing to urge the negotiators of the Anti-Counterfeiting Trade Agreement (ACTA) to immediately publish the draft text of the agreement, as well as pre-draft discussion papers (especially for portions for which no draft text yet exists), before continuing further discussions over the treaty. We ask also that you publish the agenda for negotiating sessions and treaty-related meetings in advance of such meetings, and publish a list of participants in the negotiations." See* at: http://www.wired.com/images_blogs/threatlevel/files/actaletter.pdf. [Accessed on 31.01.2013].

**35** *"The lack of transparency in negotiations of an agreement that will affect the fundamental rights of citizens of the world is fundamentally undemocratic. It is made worse by the public perception that lobbyists from the music, film, software, video games, luxury goods and pharmaceutical industries have had ready access to the ACTA text and pre-text discussion documents through long-standing communication channels."* Ibidem.

**36** A good example of such an explanation is the position of the European Commission issued in November 2008 in which it stated as follows: *"It is alleged that the negotiations are undertaken under a veil of secrecy. This is not correct. For reasons of efficiency, it is only natural that intergovernmental negotiations dealing with issues that have an economic impact, do not take place in public and that negotiators are bound by a certain level of discretion." See:* European Commission, *"Fact Sheet: Anti-Counterfeiting Trade Agreement"* 23 October 2007 (Updated November 2008) available at: trade.ec.europa.eu/doclib/docs/2008/october/tradoc_140836.11.08.pdf. [Accessed on 31.01.2013].

**37** European Parliament resolution of 10 March 2010 on the transparency and state of play of the ACTA negotiations, available at: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2010-0058&language=EN&ring=P7-RC-2010-0154 [Accessed on 31.01.2013].

**38** Such agreements are often made between the ISPs and the representatives of copyright holders or the collecting societies. They are usually negotiated in secret, and information about them most often leaks to the public through unofficial sources, causing discontent or even indignation on the part of the general public. A good example of such an agreement is the Polish draft agreement, "*On cooperation and mutual assistance in the protection of intellectual property rights in the digital environment,"* negotiated between the representatives of collecting societies and ISPs under the auspices of the Polish Ministry of Culture, which was finally blocked by the NGOs claiming it would endanger the fundamental right to privacy.

**39** *See:* Lessig, L. *Remix: Making Art and Commerce Thrive in the Hybrid Economy*, Penguin Press, New York, 2008.

**40** *See:* Lehman, B. *Intellectual Property and the national Information Infrastructure: The Report of the Working Group on Intellectual Property Rights*, Darby: Diane Publishing, 1995 quoted after: Lawrence Lessig, Remix, *op. cit*. p.39.

**41** *See:* Mook, N. "RIAA Sues 261, Including 12-Year-Old Girl," *BetaNews,* 09.09.2003, available at: http://betanews.com/2003/09/09/riaa-sues-261-including-12-year-old-girl/ [Accessed on 31.01.2013]; Mook, N. "RIAA Sues Deceased Grandmother," *BetaNews*, 04.02.2005, available at: http://betanews.com/2005/02/04/riaa-sues-deceased-grandmother/ [Accessed on 31.01.2013].

**42** *See especially:* Judgement of 16.09.2011 *Sony BMG Music Entertainment vs. Joel Tenenbaum,* United States Court of Appeals for the First Circuit, Nos. 10-1883-10-1947, 10-2052, already quoted before, in which the court obliged a minor to pay damages in amount of $ 675,000 for the infringement of copyright through the act of illegal *file-sharing*, available at: http://www.ca1.uscourts.gov/pdf.opinions/10-1883P-01A.pdf [Accessed on 31.01.2013].

**43** The official name of the so-called "HADOPI Law " in French is «Loi n° 2009-669 du 12 juin 2009, Projet de loi favorisant la diffusion et la protection de la création sur Internet.» *See, e.g.*: Johns, A., *Piracy: The Intellectual Property Wars from Gutenberg to Gates*. Reprint, University of Chicago Press, Chicago, 2011.

**44** *See, e.g.:* Ibidem.

**45** Ginsburg, J.C., *op.cit*., p.5.

**46** *Social norms* are here interpreted as normative statements that identify social expectations arising in the course of repeated interactions. They are enforced either through the application of internal sanctions of the *ego*, which emerge as a result of the internalisation of the norms and/or through the application of external, informal (i.e. non-legal) social sanctions. Social norms might, but do not necessarily have to, coincide with legal norms. Even if they do coincide, they belong to diverse normative systems. For a general review of sociological theories dealing with the concept of *'social norms,' see: e.g.*, Horne Christine 'Sociological Perspectives on the Emergence of Social Norms,' in Hechter Michael and Opp Karl-Dieter, *Social Norms*, (Russell Sage Foundation, 2005), pp. 3-34; *See also:* Durkheim, E. (1915) *The Elementary Forms Of The Religious Life.* Free Press, New York; Durkheim, E. (1951) *Suicide.* Free Press, New York; Durkheim, E. ([1903] 1953) 'The Determination of Moral Facts,' in Durkheim, E., *Sociology and Philosophy.* Cohen and West, ([1903] 1953), London, pp. 36- 43. For an analysis of the mutual influence between social and legal norms, *see: e.g.*, Bicchieri Ch., Jeffry R. and Skyrms B., (eds) (1997) *The Dynamics Of Norms.* Cambridge University Press, New York.

**47** Wu, T. (2003) 'When Code is not Law,' *Virginia Law Review*, Vol.89, p. 111.

**48** I applied this reasoning also in my other analyses, esp.: Gracz, K., "Bridging the gaps between the social and legal norms concerning protection of intellectual and artistic creations: on the crisis of copyright law in the digital era." *op.cit.* and Gracz, K., "Oposing Expansion of Copyright Law. Social norms in quest against ACTA and *Commodification of Knowledge and Culture Project*" in: Dimou A., and Daale C., (eds.) *Expansion of Intellectual Property in Modern Europe.* Geisteswissenschaftliches Zentrum der Universität Leipzig, Leipzig 2013 (forthcoming).

**49** This part of the analysis is strongly inspired by the article written by Prof. Tim Wu, When Code is not Law, Ibidem.

**50** *See, e.g.*: Posner, R.A., *Economic Analysis of Law*. Aspen Law & Business, New York, 1998, p. 242, where the author states: *"The model can be very simple: A person commits a crime because the expected benefits of the crime to him exceed the expected costs."*

**51** Professor Wu in his article, *When Code is not Law*, suggests that the influence of social norms on compliance has already been a topic of profound research, whereas the mechanisms of avoidance have been so far neglected. In his article he elaborates on the latter.

**52** The most basic models of compliance acknowledge the power of social norms in encouraging compliance with law; however the reverse process of the discouraging effect in the situation of conflicts between law and legal norms should not be undervalued.

**53** *See:* Tim Wu, *op. cit.* pp.112-116.

**54** Ibidem.

**55** Wilson, J.Q. *Political Organizations,* Basic Books, New York, 1973.

**56** Kollman, K. *Outside Lobbying: Public Opinion and Interest Group Strategies*, Princeton University Press, Princeton (NJ), 1998, p. 9.

**57** Culpepper, P.D., *Quiet Politics and Business Power. Corporate Control in Europe and Japan*, Cambridge University Press, New York 2011, p. 5.

**58** Ibidem, pp. 4-5.

**59** Ibidem, p. 5.

**60** Ibidem, generally.

**61** Ibidem, generally.

**62** Ibidem, p.10.

**63** Daly A. and Farrand B., *Scarlet v SABAM: Evidence of an Emerging Backlash Against Corporate Copyrights Lobbies in Europe?* (May 14, 2012), available at SSRN: http://ssrn.com/abstract=2095295, p. *9.* [Accessed on 31.01.2013].

**64** One of the plausible explanations of this fact, which I develop in my PhD project, stems from the historical analysis of the development of Polish social norms with regards to access to knowledge and culture, which proves that due to historical experience, Poles support open access to cultural and knowledge goods much more than Western-Europeans. For more details *see also*: Gracz. K., *Bridging the norms... op.cit.* Another reason might be the shape of the Polish Copyright Law currently in force, with its considerably liberal approach to permissible private use that undoubtedly shapes expectations of the general public as to the wide access to cultural goods within the scope of legal use, and as such may partially explain why the anti-ACTA movement started in Poland and why it was in this country that ratification of the Treaty triggered such a strong resistance. For the potency of copyright regulations is not limited to the direct normative plan and the bare legal operations but it *"also stems from the power of legal rules to determine discourse, which in turn determines thought,"* as it was aptly stated by Prof. Neil Natanel. *See:* Netanel, N. *"Copyright Alienability Restrictions and the Enhancement of Author Autonomy: A Normative Evaluation," 24 Rutgers L.J. 347, 1993, p. 442.*

**65** Tyler, T.R. *Why People Obey the Law.* Yale University Press, New Haven and London, 1990, p. 7.

**66** Tyler, T.R. *The psychology of Procedural Justice, in: Why People...* op.cit. pp. 115-125.

**67** Ibidem. *See also*: *http://en.wikipedia.org/wiki/Procedural_justice#The_participation_model* [Accessed on 31.01.2013].

**68** Netanel, N. "Why has Copyright Expanded. Analysis and Critique" in: *6 New Directions in Copyright Law*, MacMillan, F. (ed.), Edward Elgar, Cheltenham, UK; Northampton, MA, USA, 2008, p. 5.

**69** E.g. Trevor Clarke, Assistant Director General for the Culture and Creative Industries Sector of WIPO, *see:* Ermert, M., "Multi-Stakeholder Discussions á la Internet Governance Forum For WIPO?" in: *Intellectual Property Watch*, 8.11.2012, available at: http://www.ip-watch.org/2012/11/08/multi-stakeholder-discussions-a-la-internet-governance-forum-for-wipo/?utm_source=daily&utm_medium=email&utm_campaign=alerts [Accessed on 31.01.2012].

# Patentability and Scope of Protection for DNA Sequence-Related Inventions from the Perspective of the United States of America and Europe

by **Radoslav M. Milkov***
LL.B. Candidate at The Hague University of Applied Sciences (The Hague, The Netherlands)

**Abstract:** Since the mapping of the human genome and the technical innovations in the field of biotechnology, patent law has gone through great controversies. Protection is required for an investor to make an investment but how broad should the given protection be? Whether the invention is a micro-organism capable of dissolving crude oil, or the gene of a soya plant, the genetic engineering required for their production entails vast amounts of capital. The policy in that respect is tailored by legislative acts and judicial decisions, ensuring a fair balance between the interests of patent right holders and third parties. However, the policy differs from jurisdiction to jurisdiction, thus creating inconsistencies with regards to the given protection to the same invention, and as a result this could deter innovation and promote stagnation.

The most active actors shaping the patent policy on an international level are the patent offices of the United States of America, Japan and the European Patent Organization. These three patent offices have set up a cooperation programme in order to promote and improve efficiency with regards to their patent policies on a global scale. However, recent judicial developments have shown that the policy in respect to the field of biotechnology differs between the patent regimes of the United States of America and the two-layer system of the European Patent Organisation/ the European Union.

**Keywords:** Patent; DNA Biotechnology; Patentability Requirements; Scope of Protection; US Patent Regime; European Patent Regime



Recommended citation: Radoslav M. Milkov, Patentablility and Scope of Protection for DNA Sequence-Related Inventions from the Perspective of the United States of America and Europe, 4 (2013) JIPITEC 36, para. 1.

## A. Introduction

1 The debate regarding patents for biological material has intensified in the past forty years, resulting in high publicity and wide media coverage in the field of biotechnology.[1] The term *biotechnology*, for the purposes of this Research Paper, should be understood to mean "any technological application that uses biological systems, living organisms, or derivatives thereof, to make or modify products or processes for specific use."[2] Moreover, biotechnology is not a newly developed concept, but it is one of the first sciences developed by mankind.[3] The high publicity and media coverage mentioned above is a new feature for the field, and has resulted in a wide public awareness of experimentation and testing carried on living organisms in the name of technological development and medical progress.

**2** Furthermore, this technological development and medical progress has been facilitated through patent systems. The "primary purpose of the patent system is to provide incentives for the disclosure of valuable inventions that might otherwise be kept secret. [The society] offers a bargain: a limited period of statutory exclusivity for the claimed invention in exchange for full disclosure of the invention."[4]

**3** Additionally, without the negative monopoly rights for industrial exploitation provided by a patent, the majority of investors would hardly devote any resources if there is no guarantee that their investment would be secured in the end. This being said, then the research and development within heavy capital-intensive fields such as the one of biotechnology, would become stagnant if there was no adequate protection.

**4** Thus, these *ownership* rights sparked the debate forty years ago concerning patents upon biological material. The debate was concentrated around the questions of whether or not "life" could be owned or whether these negative monopoly rights could amount to a modern form of slavery.[5] In that regard, "many advocates have ... declared deoxyribonucleic acid [hereinafter "DNA"] to be common to the global human heritage."[6] However, currently it is widely accepted that biological patents are vital for the development of modern medicine and bioresearch, leading to the debate's development. "The debate today has seen a shift in focus, from questioning the possibility to patent ... DNA-related inventions ... [to questioning] the strength of the patents and the type of protection those inventions receive."[7]

**5** The purpose of this descriptive Research Paper is to examine the patentability and scope of protection for DNA sequence-related inventions from the perspectives of the United States of America and Europe. Moreover, it should be noted that the "DNA is considered to be a chemical substance, and consequently, the basic patent law principles applicable to chemical inventions will equally be applicable to DNA inventions."[8]

**6** In Part B of this Research Paper, the author will examine the bio-patent policy from an international perspective. This will be followed by a discussion in Part C on the patent systems of both the United States and Europe, with an emphasis upon their respective jurisprudences concerning the patenting of DNA material.

**7** Afterwards, this Research Paper will turn in Part D to an examination of certain specific issues related to the patentability of DNA sequences. First, it will be considered whether innovations in the field of biotechnology could be categorized as inventions, or non-patentable discoveries. This will be followed by a discussion on the criterion of *novelty* in respect to DNA sequence innovations. Afterwards, it will be considered whether the DNA sequence patents could fulfil the criterion for *inventive step/non-obviousness*. At the end of Part D, an examination on the *industrial applicability/utility* for DNA sequence inventions will be offered.

**8** In Part E of this Research Paper, the author will turn to the issue of the scope of protection for DNA sequence-related patents and will elaborate upon the four main types of patents: product based patents, process based patents, use based patents and purpose-based patents.

**9** In Part F of this Research Paper, the author will present a conclusion in light of the analysis that has been given.

## B. Introductory remarks of the bio-patent policy from an international perspective

**10** The validity and scope of a patent depends on the jurisdiction that grants it. This means that a patent granted by the United States Patent and Trademark Office (hereinafter "USPTO"), is applicable only within the jurisdiction of the United States. This could have a negative impact upon the decision of an inventor to disclose his or her invention if protection is not provided in other jurisdictions as well.

**11** Organisations such as the European Patent Office (hereinafter "EPO") or the World Intellectual Property Organisation (hereinafter "WIPO") give a solution to this problem, through the administration of the European Patent Convention[9] (hereinafter "EPC") and the Patent Cooperation Treaty[10], respectively.

**12** They provide the possibility to an inventor to apply for multiple patents within the jurisdictions of their respective Member States using a single application form. It should be noted that these organisations do not grant a single patent with unitary effect, but rather a bundle of domestic patents for which the inventor has applied.

**13** There has been a discussion[11] for many years about the creation of a unitary patent for the European Union similar to the truly regional patent of the African Intellectual Property Organization (hereinafter "OAPI").[12] The negotiations in that regard culminated with the adoption of two Regulations through enhanced cooperation,[13] and the adoption of an Agreement on a Unified Patent Court (hereinafter "the Agreement").[14] The ambition behind these pivotal steps is to make the internal market of the European Union more competitive on the global technology scale.

**14** It is interesting to note that, "as things now stand, an applicant seeking patent protection throughout the entire territory of the [European Union] ... will ... have to obtain a combination of a European patent with unitary effect and national and/or European patents. This is so because Spain and Italy do not participate in the enhanced cooperation in the area of the creation of unitary patent protection and, therefore, a unitary patent will at best cover the territories of only 25, but not all, EU Member States."[15]

**15** The above-mentioned Regulations will be applicable either on the 1st of January 2014 or the date of entry into force of the Agreement, whichever is the later.[16] Moreover, the Agreement enters into force either on the 1st of January 2014 or four months after the thirteenth state has ratified it, and among those thirteen Member States it is required that France, Germany and the United Kingdom are present. [17]

**16** "Globally, the EPO, USPTO, and Japanese Patent Office [hereinafter "JPO"] are the most influential actors in [the] international patent policy, and regularly meet in trilateral discussions."[18] Furthermore, intellectual property law is being enforced and applied primarily at the national level. This means that an international framework should outline this level in order to avoid discrepancies within the many national patent regimes. In that regard, WIPO plays a vital role for the administration of various intellectual property Unions and international agreements related to intellectual property law. [19]

**17** The Agreement on the Trade-Related Aspects of Intellectual Property Rights (hereinafter "TRIPS"),[20] is an agreement that was adopted under the auspices of the World Trade Organisation (hereinafter "WTO"). TRIPS incorporates within itself many of the provisions covered by the Conventions administered by WIPO. Moreover, it primarily provides that the Members of the WTO are obliged to follow a minimum standard of protection for intellectual property rights.

**18** With regards to the patentability of DNA inventions, TRIPS is *silent*. Its Member States are not obliged explicitly to grant protection for DNA-related inventions. However, Article 27(3)(b) of TRIPS does not refer to DNA sequence inventions as an *exception* to patentability. Accordingly, it gives the Member States a wide margin of discretion with regards to the patentability of DNA in respect to the patentability criteria and excludability from patenting.[21]

**19** A discussion concerning exactly this discretion will be provided within Part C of this Research Paper, namely in respect of the patent regimes of the United States and Europe. Before examining them separately in detail, it is required to be noted that the United States follows the doctrine of *first-to-invent* while in Europe the doctrine of *first-to-file* is the predominant one. The difference is that in the United States, the patent holder has to prove that he or she invented the DNA-related invention first in case of infringement proceedings, while in Europe all that matters in infringement proceedings is who filed the application first.

**20** On a more recent note, the patent system in the United States will change from *first-to-invent* to *first-inventor-to-file* in 2013.[22]

## C. Bio-patents from the perspectives of the United States and the European patent regimes

### I. The jurisprudence in the United States with regards to Biotechnology

**21** Under the Constitution of the United States of America, the Congress has the power "to promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries."[23]

**22** The USPTO, mentioned above, is a federal administrative body established by the U.S. Patent Act, with the task of administering the U.S. patent system.[24] Under the U.S. Patent Act, there are four requirements with equal legal value, which an invention needs to fulfil in order to be granted a patent.[25] These requirements are: the invention must be of a patentable subject matter,[26] it must be novel,[27] it must have to have utility,[28] and it must be non-obvious.[29]

**23** With regards to biotechnology, the patent regime of the United States could be said to be fairly liberal. *The debate* that was discussed in the introductory part of this Research Paper goes far beyond the question of whether or not "life" itself could or should be patented in the United States. As Chief Justice Burger noted, the relevant distinction in the field of biotechnology should be "not between living and inanimate things, but between products of nature, whether living or not, and human-made inventions."[30]

**24** In the case of *Funk Bros Seed Co. v. Kalo Inoculant Co.*,[31] the Supreme Court of the United States developed the *product of nature* doctrine. This doctrine is used to define the patentable subject-matter for an invention in the field of biotechnology. The Supreme Court held that the "manifestations of laws of nature, [are] free to all men and reserved exclusively to none. He who discovers an unknown phenomenon of

nature has no claim to a monopoly."[32] The substance of this doctrine is that a product of nature cannot be patentable since it fails to satisfy the criterion of novelty. Examples of such *products of nature* include the laws of physics, mathematical equations and all non-isolated, non-purified living matter.[33]

**25** Moreover, the case of *Diamond v. Chakrabarty*[34] marked the beginning of a new era for the U.S. patent system. The case concerned the challenging of a decision to grant a patent for a human-engineered bacterium of the Pseudomonas genus, which was able to break down crude oil and thus help treat and control oil spills.

**26** The USPTO agreed that this was a *novel* invention; however it rejected granting the patent on two grounds: (1) the micro-organism was a *products of nature* and (2) the invention was not of patentable subject-matter. Mr. Chakrabarty appealed this decision and the Board of Patent Appeals and Interferences affirmed the USPTO's conclusion on the second ground. The Board of Patent Appeals relied on "the legislative history of the 1930 Plant Patent Act, in which [the] Congress extended patent protection to certain asexually reproduced plants, [and] the Board concluded that § 101 was not intended to cover living things such as these laboratory created micro-organisms."[35]

**27** Mr Chakrabarty then appealed to the Court of Customs and Patent Appeals (hereinafter "CCPA"), which reversed the decision of the Board of Appeals. In the case of *In re Bergy*[36] the CCPA had concluded that "the fact that micro-organisms are alive is without legal significance for purposes of the patent law"[37], and it took this judgement into consideration while deliberating upon the *Chakrabarty* case.

**28** In March 1980, the matter was brought before the attention of the United States Supreme Court. "Essentially, the Court held that the bacterium was altered to a sufficient extent to qualify as an invention,"[38] and thus the mutated organism fulfilled the criterion of *novelty* and was not a *product of nature*. The Supreme Court affirmed the judgement given by the CCPA on the 16th of June 1980, and on the 31st of March 1981 the USPTO issued the contested Patent.[39]

**29** Since the Supreme Court rendered this judgement, "the patent office has been granting patents over genes, animals, plants and other products of biotechnology."[40] According to statistics made by the OECD in 2002, "one study estimates that the total number of DNA patents granted by the USPTO to date is somewhere around 10 000."[41] And according to the World Survey of Genomics Research, in 2001 alone the USPTO granted over 5 000 DNA patents.[42] "In a more recent article (2005), Kyle Jenson and Fiona Murray[43] identified 4,270 US patents containing claims on human DNA sequences."[44] According to research conducted by Eric J. Rogers, the USPTO granted more than 40 000 DNA-related patents until 2011, since the *Chakrabarty* case.[45]

**30** *The debate* discussed in the introductory section of this Research Paper culminated in the resent case of *Association for Molecular Pathology v. United States Patent & Trademark Office and Myriad Genetics, Inc.*[46] The case had great potential in blocking the patentability of DNA-related inventions in the United States. "The high profile litigation brought the topic of DNA patenting into the spotlight, prompting several organizations, both domestically[47] and abroad,[48] to publish reports with policy recommendations[49]."[50]

**31** This case concerned the patentability of two particular breast cancer genes (BRCA1, BRCA2) and certain methods for testing the genetic material. Moreover, the particular issues before the Court concerned 15 claims from 7 patents.[51]

**32** Furthermore, research made by Myriad Genetics, Inc. showed that women with mutations in the above-mentioned genes were significantly susceptible to develop breast cancer. "Using positional cloning techniques, the inventors found that mutations in the BRCA genes correlate with a significantly increased risk of ovarian and breast cancer."[52] According to statistics presented by the National Cancer Institute,[53] the average American woman has 12.29% to develop breast cancer in her life. However, the statistics conducted by Myriad Genetics suggest that women with mutation in the BRCA genes are with 50-80% higher risk of developing breast cancer, and a 20-50% chance of developing ovarian cancer.[54]

**33** "This may seem like a boon for medical research, a breakthrough in humanity's endeavour to conquer cancer."[55] However, the costs of testing the genetic material protected by the contested patent made it impossible for the insurance policies of some patients to cover the amount of the test.[56] Additionally, the defendant in the case had employed an aggressive strategy with respect to the contested patent. The strategy prohibited others from making the test of the genetic material, thus ensuring that if patients wished to make a second test due to fear of human mistake, they had to do it at Myriad Genetics laboratories again. Additionally, the patent put an estoppel upon the research and development in the field concerning the BRCA genes due to the fact that researchers and medical organisations feared potential infringement litigations.[57]

**34** During the proceedings at first instance the District Court ruled that even if isolated and purified, the DNA-related inventions were still a product of nature. "It was the first time any federal court found DNA patents to be invalid for ineligible subject matter."[58] The plaintiff to the case also raised arguments with

respect the *constitutionality* of the patentability of DNA compounds.[59]

**35** However, the United States Court of Appeals for the Federal Circuit squashed the judgement of the District Court, "holding that isolated and purified DNA molecules and certain DNA-related methods are indeed patentable subject matter."[60] The Appeals Court looked at three different types of patents, namely: (1) absolute product patents, (2) purpose bound patents for the purposes of analysing and comparing natural DNA sequences and mutated DNA sequences, and (3) purpose bound patents covering more than analysing and comparing between natural DNA sequences and mutated DNA sequences.

**36** (1) With respect to the absolute product patent, Judge Lourie and Judge Moore concurred that if a DNA molecule is isolated, it is patentable subject-matter "because the covalent bonds at the ends of a DNA molecule, when isolated, must be broken, making the molecule a 'distinct chemical entity' that is by definition 'markedly different' from any DNA molecules existing in nature."[61]

**37** (2) With respect to the purpose-bound patents for the purposes of analysing and comparing natural DNA sequences and mutated DNA sequences, the Court held that it was not patentable subject-matter. This was due to the fact that *abstract mental processes*, which are involved in the analysis and comparison, would ensure that the scope of protection was too broad.[62]

**38** (3) With respect to and purpose-bound patents covering more than analysing and comparing natural DNA sequences and mutated DNA sequences, the Court held that it was patentable subject matter. This was so because the additional step that goes beyond mere analysis and comparison could lead to "potentially valuable inventive methods."[63]

**39** It is interesting to note that in the end of 2012 the United States Supreme Court expressed its willingness to adjudicate upon the case of *Myriad*.[64] It is expected that the Court will reach a decision on the matter in 2013.

**40** On a more recent note, in 2012 the United States Supreme Court ruled upon the case of *Mayo Collaborative Services v. Prometheus Laboratories, Inc*.[65] The case concerned two patents for the use of thiopurine drugs in the treatment of autoimmune diseases, such as Crohn's disease and ulcerative colitis.[66] "Stated generally, the patents claim methods of: (a) administering a thiopurine drug to a patient, and (b) determining the levels of the drug or the drug's metabolites in red blood cells in [a] patient. The measured metabolite levels are then compared to known metabolite levels. If the measured metabolite levels in the patient are outside the known range, then the physician should increase or decrease the level of drug to be administered so as to reduce toxicity and enhance treatment efficacy."[67]

**41** "Prometheus is the sole and exclusive licensee of the patents at issue. Mayo purchased and used medical diagnostic tests from Prometheus that embody the methods described in the patents. Mayo later developed and marketed its own diagnostic test, resulting in Prometheus bringing an action for patent infringement against Mayo."[68]

**42** Throughout the proceedings, the District Court found that the two contested patents were of unpatentable subject matter because they dealt with natural law - "namely the correlation between thiopurine metabolite levels and the toxicity and efficacy of thiopurine drug dosages."[69] However, in 2009 the Court of Appeals for the Federal Circuit reversed the District Court's judgement and used the "machine-or-transformation test"[70] to determine that the claims of Prometheus were patentable.

**43** In the case of *Bilski v. Kappos* in 2010, the majority of Justices in the United States Supreme Court agreed that "the 'machine-or-transformation' test should not serve as the exclusive test for determining whether a claimed method [is] patent-eligible or not."[71] For that reason the Supreme Court in the case of *Mayo v. Prometheus* vacated the decision of the Federal Circuit and ordered a rehearing of the appeal.

**44** The Court of Appeals for the Federal Circuit again held that the claims were patent eligible and Judge Lourie stated that the they were "drawn not to a law of nature, but to a particular application of naturally occurring correlations, and accordingly do not pre-empt all uses of the recited metabolite levels and drug efficacy or toxicity."[72]

**45** The Supreme Court again granted *a writ of certiorari* and disagreed with the Court of Appeals for the Federal Circuit in its decision. The Supreme Court considered that the claims set forward were directed only towards *laws of nature* and consequently were unpatentable. "The Court reviewed its precedents in order to explain that phenomena of nature and abstract concepts could not be patented because the 'monopolization of these basic tools through the grant of a patent might tend to impede innovation more than it would tend to promote it.'[73]"[74] However all inventions at some point use and apply natural laws, thus "a process is not unpatentable simply because it contains a law of nature or a mathematical algorithm"[75] and "an application of a law of nature or mathematical formula to a known structure or process may well be deserving of patent protection."[76]

**46** In its analysis, the Supreme Court stated that the claims at hand dealt with natural law, thus it was

necessary to observe whether "the patent claims add *enough* to their statements of the correlations to allow the processes they describe to qualify as patent-eligible processes that *apply* natural laws."[77] The Supreme Court identified and deliberated upon three steps that the claims added in addition to the natural law – namely: (1) an *administering step*, (2) a *determining step*, (3) and a *wherein* step.[78]

**47** (1) The *administering step* "referred simply to the relevant audience of the invention, namely, physicians who treat patients with certain diseases with thiopurine drugs."[79] In any event, the "prohibition against patenting abstract ideas 'cannot be circumvented by attempting to limit the use of the formula to a particular technological environment.'"[80]"[81]

**48** (2) The *determining step* basically refers to *any* act of measurement of the metabolite level into the blood of a patient, performed by physicians. Moreover, it was even stated in the patent applications that the methods for determination of the metabolite level in the blood were well known in the art.[82] "Thus, this step tells doctors to engage in well-understood, routine, conventional activity previously engaged in by scientists who work in the field."[83]

**49** (3) The *wherein step* "simply tells a doctor about the relevant natural laws, at most adding a suggestion that he should take those laws into account when treating his patient."[84] "According to Justice Breyer, an unpatentable law of nature does not become patentable merely by advising individuals to use the law."[85]

**50** To summarize the above-mentioned observations, the Supreme Court considered that the claims were informative to the relevant audience, the additional steps were conventional and routine, and "when viewed as a whole, add[ed] nothing significant beyond the sum of their parts taken separately."[86] For those reasons the Supreme Court concluded that, "the steps are not sufficient to transform unpatentable natural correlations into patentable applications of those regularities."[87]

**51** Additionally, the Supreme Court deliberated upon the case at hand in light of existing precedents dealing with the issue of patent eligibility of processes that embodied the equivalent of natural laws - namely the cases of *Diehr*[88] and *Flook*[89]. "The Court concluded that the claims at issue in [*Prometheus*] present a case for patentability that is weaker than the claim in *Diehr* and no stronger than the claim in *Flook*, emphasizing that the steps and wherein clauses of *Prometheus'* claims 'add nothing specific to the laws of nature other than what is well-understood, routine, conventional activity, previously engaged in by those in the field.'"[90]"[91]

**52** Throughout the course of the proceedings, the U.S. Government raised an argument that "virtually any step beyond a statement of a law of nature itself should transform an unpatentable law of nature into a potentially patentable application sufficient to satisfy §101's demands."[92] Under this argument, other requirements like *novelty* and *non-obviousness* would have a more significant impact during patent examination. However, the Supreme Court decided that this approach was not consistent with prior law, and would make the *natural law* exception to patentability virtually hollow.[93]

**53** The Supreme Court also responded to concerns that a decision against *Prometheus* could discourage diagnostic research.[94] "Justice Breyer observed that other interested parties had asserted that patents claiming the body's natural responses to illness and medical treatment should not be granted because they might limit physician access to critical scientific data. In view of these competing views, the Court was reluctant to depart from precedent denying patents on natural laws."[95]

**54** The case of *Mayo v. Prometheus* represents the willingness of the otherwise *fairly liberal* patent regime of the United States to draw a clear line between what is patentable and what is not, by elegantly defining the *law of nature* exception.

## II. The jurisprudence in Europe with regards to Biotechnology

**55** "The European patent system displays a disciplined yet inclusive regime of according patent rights to biotechnology and its numerous progenies."[96] The two primary sources that are relevant for the patentability of biotechnology within Europe are the EPC,[97] and the Biotechnology Directive 98/44/EC[98] (hereinafter "the Biotech Directive"). The scope of application of the EPC coverers all of its signatory and extension states,[99] while the Biotech Directive is applicable only within the European Union.[100]

**56** The Biotech Directive was adopted in July 1998 and it was supposed to be implemented by the 30th of July 2000; though it was done so in March 2006 after the Grand Duchy of Luxembourg became the last Member State to implement it.[101] However, on 19th of October 1998, the Dutch Government brought an annulment action before the European Court of Justice with respect to the Biotech Directive and the claim was rejected.[102]

**57** Furthermore, in 1999, through a decision of the Administrative Council, a new "Chapter IV" was inserted into Part II of the Implementing Regulations of the EPC entitled "Biotechnological Inventions". It contained four rules that are in accordance with

the Biotech Directive.[103] This amendment to the Implementing Regulations serves as a supplementary interpretation of the patentability of biotechnology within the EPC, which gives additional clarification by providing clear exceptions.[104]

**58** The EPC has a fourfold cumulative criterion for determining whether an invention is patentable-namely, the requirements of patentable subject matter[105], novelty,[106] inventive step,[107] and industrial application.[108] "These four criteria were reaffirmed in [the Biotech Directive]. In fact, for the purposes of ensuring compatibility between the EPC and the bio-patents, [the Biotech Directive] categorically under Article 3.2 specifies that biological material, after considerable human processing and intervention, cannot be precluded from the ambit of patent protection simply because its initial existence was inherent in nature."[109]

**59** A clear distinction between the European and the U.S. patent regimes is the *public order and morality* exception from patentability. Under Article 53(a) of the EPC, any invention that is against the public order or morality is barred from gaining patent protection, while in the U.S. there is no such exception.

**60** The EPO Board of Appeals in the case of *Plant Cells/ Plant Genetic Systems*[110] has defined the notions of *Public Order* and *Morality*. According to the Board of Appeals, public order "covers the protection of public security and the physical integrity of individuals as part of society"[111] while it also encompasses the protection of the environment. Moreover, the concept of morality has been defined as "... related to the belief that some behaviour [is] right and acceptable whereas other behaviour [is] wrong, this belief being founded on the totality of the accepted norms which [are] deeply rooted in a particular culture. For the purposes of the EPC, the culture in question [is] defined as the culture inherent in [the] European society and civilisation. Accordingly, inventions the exploitation of which [is] not in conformity with the conventionally accepted standards of conduct pertaining to this culture [are] to be excluded from patentability as being contrary to morality."[112]

**61** The Decisions in *Hormone Relaxin*[113] and *Harvard Onco-mouse*[114] provide clear examples of the willingness of the European patent regime to grant patents to biotechnological inventions. Additionally, those decisions illustrate how the EPO deals with situations in which, the subject-matter concerned could be viewed initially as contrary to public order and morality.

**62** The *Hormone Relaxin* case limited the *product of nature* doctrine. It involved a DNA-sequence patent for the process of the creation of one specific protein. However, it was contested that the process of isolation lacked inventive step. EPO held that the subject matter in this case was more than a mere discovery; thus it involved inventive step because the protein had to be isolated from its surroundings and a process had to be developed to obtain it.[115] The controversy surrounding this case was the fact that it dealt with human tissue, in particular the DNA of pregnant women. However, "once extracted and treated, [the DNA] was characterised, not as 'life', but as substance carrying genetic information which can be used to produce proteins that are medically useful. The patent grant was therefore maintained."[116]

**63** The *Harvard/Onco-mouse* case involved a genetically modified organism - a non-human mammal, in particular a mouse, which had an oncogene that made it highly susceptible to the growth of breast cancer cells, making it a useful subject for Onco-research. This organism was engineered at Harvard Medical School in the laboratory of Dr. Philip Lader and Dr. Timothy A. Stewart. At first, the scope of the controversial patent was for a method of producing transgenic non-human mammals, but through the course of proceedings, the scope was narrowed to a method of producing transgenic rodents containing an additional cancer gene.[117]

**64** Harvard College applied for patent protection for the abovementioned method before The Examination Division of the European Patent Office, which deliberated and later rejected the application. The grounds for rejection were that the organism was a non-patentable invention, its subject-matter was *an animal variety* and that patent law was not the right legislative tool for regulating issues related to genetic engineering.[118]

**65** "On appeal, the Technical Board of Appeals held that the Examining Division had misconstrued the exclusion, which being an exception to patentability, ought to be construed narrowly.[119] Importantly, the Board of Appeal said that Article 53 (b) [EPC] did not exclude animals *in general*"[120] from patentability. Moreover, there were compelling reasons to deliberate, upon the implications for patentability stemming from Article 53 (a) EPC.[121] Furthermore, the Technical Board of Appeals considered that the genetic engineering of animals was problematic in several respects, namely that it caused suffering towards the test subjects and the possibilities of exposing the outside environment to those test subjects.[122] It was considered that this could lead to unforeseeable and irrevocable repercussions.

**66** For the abovementioned reasons, the Technical Board of Appeals construed a *balancing test*: "The decision as to whether or not Article 53(a) EPC is a bar to patenting the present invention would seem to depend mainly on a careful weighing up of the suffering of animals and possible risks to the environment on the one hand, and the invention's

usefulness to mankind on the other. It is the task of the department of first instance to consider these matters in the context of its resumed examination of the case."[123]

**67** The case was remitted to the Examination Division, which identified three interests that needed to be taken into account while deliberating upon the case at hand in light of the above-mentioned balancing test. Those three interests were, firstly the interest of humankind to remedy widespread and dangerous diseases; secondly the protection of the environment from the uncontrolled dissemination of unwanted genes; and thirdly the avoidance of cruelty to animals.[124]

**68** "The Examination Division concluded that upon balancing the various considerations, the Oncomouse invention was of great benefit to mankind, would limit the number of animals used for cancer research ... and that the risk of escape was minimal."[125] Moreover, "of the advantages of the invention, the animals were considered highly useful in a form of experimentation indispensable to medical research. It was the importance of this consideration which justified the patent grant."[126]

**69** On a more recent note, the European Court of Justice sat in Grand Chamber in 2010 over a case with tremendous impact upon the patentability of DNA-related inventions in Europe. The case of *Monsanto Technology LLC v. Cefetra BV and Others*[127] concerned a European Patent granted in 1996 for a DNA sequence that was inserted into a Soya bean plant,[128] making it resilient and non-sensitive to commonly used herbicide.[129]

**70** The factual situation of the case is as follows: the Argentinian company Monsanto owned the above-mentioned European Patent but did not have a patent in Argentina. Three European companies, Cefetra, Vopak and Toepfler, imported soya meal into the internal market of the European Union, containing the protected DNA sequence within their products. Monsanto brought infringement proceedings before a Dutch Court, which later referred four questions to the European Court of Justice.

**71** The first question concerned the interpretation of Article 9 of the Biotech Directive. The Dutch Court essentially asked whether Article 9 confers patent protection rights, even if the protected DNA sequence stopped performing its designated function but could resume performing it, if it is inserted into the cells of a living organism.[130] Thus, the question was principally whether Article 9 of the Biotech Directive provides for an absolute product protection.[131]

**72** The European Court of Justice stated "that the protection provided for in Article 9 of the Directive is not available when the genetic information has ceased to perform the function it performed."[132] Moreover, the Court completely rejected the argument of Monsanto concerning the absolute product protection,[133] stating that through textual interpretation of Article 9, the protection it provides is closely linked and conditional to, the functionality of the DNA sequence concerned.[134]

**73** The second question raised by the Dutch Court essentially concerned the scope of the Directive.[135] In particular whether Article 9 effects an exhaustive harmonisation of the protection it confers, precluding national legislation, which grants absolute product protection.

**74** The European Court of Justice analysed the recitals of the Directive, concluding that the legislature's intention was to ensure an equal level of protection for patents in all Member States.[136] Leading to the conclusion that "the Directive effects an exhaustive harmonisation in the European Union, with the result that it precludes national legislation offering absolute protection to a sequence of DNA as such, regardless of whether it performs the specific function for which it was patented."[137]

**75** The third question raised by the Dutch Court essentially referred to the temporal scope of the Directive.[138] In particular whether the Directive's scope extends to patents granted prior to its adoption.

**76** The European Court of Justice held that, "Article 9 of the Directive precludes the holder of a patent issued prior to the adoption of that directive from relying on the absolute protection for the patented product accorded to it under the national legislation then applicable."[139]

**77** The fourth question raised by the Dutch Court essentially asked whether Articles 27 and 30 TRIPS[140] affected the interpretation of Article 9 of the Biotech Directive.[141]

**78** The European Court of Justice affirmed that the provisions under the TRIPS Agreement did not have direct effect,[142] and held that the given interpretation of Article 9 of the Biotech Directive did not run counter to the obligation imposed by TRIPS[143] and "that Articles 27 and 30 of the TRIPS Agreement do not affect the interpretation given of Article 9 of the Directive."[144]

# D. Analysis of specific issues relating to patenting DNA sequences

## I. Invention or Discovery?

**79** Before analysing this topic, the terms of *discovery* and *invention* must be defined. A "*discovery* is the unearthing of causes, properties or phenomena already existing in nature; *invention* is the application of such knowledge to the satisfaction of social needs."[145] One of the issues with regards to *the debate* described in the introductory section of this Research Paper was that a living organism could be only discovered and not invented. The rationale behind this is that there must be a distinction between patentable inventions and unpatentable discoveries. In the field of biotechnology, and in particular DNA sequence research, however, sometimes this distinction is not that clear.

**80** The approach taken by the EPO is different from the one taken by the USPTO in respect to the distinction of *invention* and *discovery*. The United States Code does not make an explicit distinction between the two. However, in practice, natural phenomena are excluded from patentability.[146] Moreover, the recent developments in the case of *Prometheus*,[147] in which the United States Supreme Court clarified the *law of nature* exception of patentability, actually blurred the distinction between *discoveries* and *inventions* in the United States. However, under the EPC, the question of *invention* versus *discovery* is explicitly answered. Discoveries are of unpatentable subject matter, thus they have a detrimental effect upon a patent applicant.

**81** Moreover, the Biotech Directive also refers to both *unpatentable discoveries*,[148] and *patentable inventions*.[149] In the case of DNA sequence-related inventions, the claimed patents are not naturally occurring phenomena. This is so because with patenting in the field of biotechnology, the rights that are asserted are not over DNA sequences that occur naturally, but rather for DNA sequences that have been isolated and purified. The rationale behind this is that "although these DNA sequences do in fact match the sequences of our genes, they are only patented in the context of molecules which have been artificially created by cloning and are isolated from the human body."[150]

**82** The notion of *isolation* was clarified by a joint statement made by EPO, USPTO and JPO in 1988 stating that, "purified natural products are not regarded under any of the three laws as products of nature or discoveries because they do not in fact exist in nature in an isolated form. Rather, they are regarded for patent purposes as biologically active substances or chemical compounds and eligible for patenting on the same basis as other chemical compounds."[151] "Although this statement was made before the question of patenting genes came into the forefront of [*the debate* discussed in the introductory section of this Research Paper], it is consistent with the positive approach taken by these three Patent Offices on the subject of gene patents."[152]

## II. Novelty with regards to DNA sequences-related inventions

**83** This patentability requirement refers to the fact that an invention must not be known to the world before the patent application was lodged. With regards to the patent regimes of the United States and Europe, the major difference in this respect is that in the United States, there is a *grace period* of one year and in Europe there is no such thing.

**84** With respect to DNA sequence related-inventions, for example, the human genome or the human DNA are already existent in nature and thus cannot be patented. However, an isolated sequence that is the result of a technical process is patentable.[153]

**85** Moreover, the existence of a DNA sequence in a DNA library is not destructive for the element of *novelty*, given the fact that this sequence was not freely available to the public.[154] Furthermore, "it is established patent practise to acknowledge novelty for a natural substance that has been isolated for the first time and which had no previously recognised existence."[155]

**86** For the sake of an academic argument, let's consider that a DNA sequence existent in nature, even if isolated, cannot be patented due to a lack of novelty.[156] Yet, the process that creates an identical DNA sequence that is already in existence in nature is patentable *per se*. Pursuant to the general principles of patent law, in conjunction with Article 64(2) EPC, lead to the conclusion that the protection provided to a process by a patent extends to the product stemming from that process.[157] This is so because "individual [DNA sequences] in their natural state are not directly accessible and additional work is required to isolate them."[158]

**87** If the novelty of an isolated DNA sequence that is of patentable subject-matter has been proven, then an examination of the inventive step/non-obviousness and the industrial application/utility is required to be made for a patent to be granted.

## III. The inventive step/non-obviousness and DNA sequence-related inventions

**88** This patentability requirement refers to the fact that an invention must not be obvious to a person proficient in the state of the art. "When considering whether an invention is obvious, [the respectful authority] views the invention through the eyes of a notional interpreter equipped with the attributes, skills, background knowledge, and qualifications relevant to the field in which they work."[159] The qualification, skills, knowledge, *et cetera*, of the person proficient in the state of the art are dependent upon the technical field within which the invention belongs. However, for the sake of clarity this *artificial* person is not held to the standard of a Nobel Prize Laureate level of skilfulness, but should be sufficiently proficient in the concerned state of art.[160]

**89** As already stated in the introductory section of this Research Paper, the DNA sequence is simply a chemical compound and as such, the patent law principles applicable to the field of chemistry are applicable to DNA sequences as such. For that reason, the principle that the preparation of a chemical compound given that it is not new in structure is considered to be non-inventive, and applies *mutatis mutandis* to the field of DNA sequence patenting.

**90** The competent authorities in Europe and the United States differ in their application of the *inventive step/non-obviousness* requirement. In the United States, following the judgement of *In re Deuel*, a DNA sequence is *prima facie* non-obvious if it is structurally different from one already existent in nature.[161] Moreover the amount or methodology of work put into the characterisation of the DNA sequence is irrelevant for the purposes of this patentability requirement.[162] Furthermore, "many have argued that technological advances in DNA sequencing now mean that the process of isolating a gene can no longer be regarded as inventive,"[163] but so far the patent policy in the United States does not take those considerations into account.

**91** The patent regime of the United States has a low threshold with respect to the *non-obviousness* requirement. Even if the nature and function of a DNA sequences has been established through the usage of trivial means, such as with *in silico* techniques,[164] this does not preclude the eligibility of the DNA sequence under the requirement of *non-obviousness*.[165]

**92** The approach followed by EPO, on the other hand is more restrictive. Structural non-obviousness is not sufficient enough, thus requiring an inventive method for isolation[166] or unexpected or surprising features of the end product.[167] Moreover, an isolated DNA sequence could lack inventive step if it is structurally related to a natural DNA sequence with a known function.[168]

## IV. Industrial applicability/ utility of DNA sequences-related inventions

**93** This patentability requirement refers to the fact that an invention must be capable of being applied in any field of industry. It is considered that *Industrial Application* and *Utility* are two concepts that are highly equivalent.[169]

**94** However there are differences between the two notions that have been elaborated upon by the Standing Committee of the Law of Patents of WIPO in 2003.[170] An invention is considered to be *industrially applicable* "if it can be made or used in any kind of industry, including agriculture. [Moreover] the general understanding is that the term "industry" shall be interpreted in the broadest possible sense."[171] In respect to the field of biotechnology, Article 5.3 of the Biotech Directive states that, "the industrial application of a sequence or a partial sequence of a gene must be disclosed in the patent application."[172] Furthermore, with regards to DNA sequences, Recital 23 of the Biotech Directive states that, "a mere nucleic acid sequence without indication of a function does not contain any technical information and is therefore not a patentable invention."[173]

**95** Under the patent regime of the United States of America, the main tool that the USPTO uses in order to examine an invention in light of this patentability requirement is the Utility Examination Guidelines.[174] Under those guidelines it is stated that an invention has to demonstrate a "specific, substantial and credible utility."[175] "The term *credible* is interpreted ... as meaning that the usefulness claimed for the invention must be theoretically possible, even though it may not have been demonstrated in the claims."[176]

**96** Industrial applicability/utility, in particular, have a very specific feature in regards to the field of biotechnology. In respect to *the debate* discussed in the introductory section, it was argued that if this patentability requirement was not interpreted strictly, patents may be granted in a fairly liberal manner - meaning that a patent could be granted on biological products without a specific *use*, barring competitors within a field from taking research initiatives.[177] The rationale behind this notion is that, "the purpose of granting a patent is not to reserve an unexplored field of research for an applicant."[178]

**97** "Even if a credible utility is stated in a patent, if further novel and non-obvious uses for a DNA

sequence are found, patent law provides that a [absolute] product patent on the sequence will extend to cover the new uses, despite their not being specified in the original patent."[179]

# E. Scope of protection for DNA sequence patents

## I. Introductory remarks

**98** The scope of a given patent defines the exclusivity of the rights it confers. Moreover the "scope of protection can influence the viability of a specific line of research."[180] For this reason, the question of how broad or narrow the protection given by a patent should be is of primary importance.

**99** The fact that, within the field of biotechnology, a patent is granted for living matter possibly capable of reproduction is a clear example of how necessary it is to define the broadness or narrowness of the scope of protection.[181] If that living matter reproduces, the next generation could have the genetically modified genes of the previous one.[182] Thus, the controversial question that arises is should the scope of the protection be extended towards the offspring of a genetically modified organism as well?[183] "There has been considerable controversy in the literature on this subject, particularly for the cases of plants and animals. It suffices here to say that patent protection indeed extends to the further generation animals and plants if the genetic information is still present in the further generations and performs its function."[184]

## II. Different types of Patents

**100** There are four main types of patents, which have differentiating characteristics. These types of patents are absolute product patents, process based patents, use based patents and purpose bound patents.

**101** The absolute product patent is a patent on the substance of an invention *per se* - the product derived. The rights granted to this type of patents cover all uses of the protected product. The term *product* in the field of DNA sequence patents is understood to mean "a chemical or biological entity, substance or composition[185] (as distinct from a device or electrical circuit)."[186]

**102** The process based patent is a patent that grants certain rights upon a method, technique or process. The rights granted under this patent may also cover the product directly derived from it. However, if the same product is achieved through another method, technique or process any claims for infringement of the first process based patent cannot be raised.

**103** The use based patent is a patent that grants rights upon the specific use of a product. "An exception [to the use based patent are the] first medical use patents. [The first medical use patents] are patents on products that are not novel in themselves, but for which no medical use has been previously described. This kind of patent exists only under European patent law. The claims cover manufacture of the known product for all medical uses."[187]

**104** The purpose bound patent is a patent that grants rights upon a product for a specific purpose. The rights derived from this type of patent cannot protect the right holder of uses outside of the specified purpose.[188] "The purpose-bound protection is a product patent and should not be confused with the use patent, the use patent does not provide any protection over the product as such but only for the [specified] use ... whereas the purpose-bound product protection protects the actual product but [it] is limited to the disclosed purpose."[189]

**105** From the four types of patents, the ones that could confer protection over the DNA sequences as such, are the absolute product patent and the purpose bound patent. For that reason, the author of this Research Paper will focus his analysis upon these two types of patents.

### 1. Absolute product patent

**106** In the case of *Diamond v. Chakrabarty*, discussed above, the applicant tried[190] to register not only the process with which the contested bacterium was created, but also the particular use of the bacterium and the bacterium *per se*. "The fact is of interest here because the claim for using the bacterium was granted in just two years, whereas the claim on the bacterium *per se* [took] almost nine years to be granted."[191] This shows the reluctance of the otherwise liberal United States patent regime to grant negative monopoly rights for industrial exploitation over genetically modified products *per se*.

**107** The notion of absolute product based patents in the field of biotechnology is relatively new. However, as already stated, DNA is considered to be a chemical compound and as such the principles governing the patenting in chemistry are applicable to it. One of the very first known absolute product based patents for a chemical invention has its origins in the United States of America shortly after the Second World War. On the 9th of May 1950 the USPTO granted an absolute product patent for the chemical of penicillin.[192]

**108** As it was discussed in Part C of this Research Paper, the notion of an absolute product patent was put under judicial scrutiny recently in the cases of *Association for Molecular Pathology v. United States Patent & Trademark Office*[193] and *Monsanto Technology LLC v. Cefetra BV and Others*.[194] Both cases dealt with the issue concerning the scope of protection for patents granted in the field of biotechnology.

**109** In the United States currently, absolute product based patents are permissible while in Europe the picture is much more complex. Under the case-law of EPO, "[i]t is generally accepted as a principle underlying the EPC that a patent which claims a physical entity *per se*, confers absolute protection upon such physical entity; that is, wherever it exists and whatever its context (and therefore for all uses of such physical entity, whether known or unknown)."[195]

**110** However, according to the interpretation given by the European Court of Justice, the protection granted by Article 9 of the Biotech Directive is exhaustively harmonising within the European Union and cannot provide protection to DNA absolute product patents.

### 2. Purpose-bound patent

**111** "The most suitable and most advocated alternative to the absolute product patent protection is the purpose-bound protection, which in contrast to the absolute product patent would extend no further than the use disclosed in the application."[196] The scope of this type of patent is confined within the *specified* use, thus other uses not listed or that fall outside of the disclosed purpose could be claimed by other applicants.

**112** This type of patent has an interesting implication for the field because a single purified DNA sequence could be subject to protection for many right holders. Since the European Court of Justice has interpreted that the Biotech Directive does exhaustively harmonise the level of protection in all Member States to purpose bound patents, it would be interesting to observe the development of biotechnologies and bioresearch in Europe. This policy decision could either promote the research and development in the field of DNA related inventions, or it could simply deter it.

## F. Conclusion

**113** The patent regimes of the United States of America and Europe do not resemble much. The policy choices made in constructing those regimes seem fairly different, however, they reach the same conclusions. Namely, that an inventor should be rewarded for his or her invention and that there should be a threshold with respect to patenting living matter.

**114** As discussed in this Research Paper, there are substantial differences with regards to the patentability requirements of DNA-related inventions. However they do not render the patent systems fundamentally different.

**115** Moreover, as recent developments have shown, the patent regimes in the United States of America, and Europe[197] have chosen different policy paths. The United States allows protection for absolute product patents while in Europe this type of patent is prohibited in the field of DNA sequences.

**116** It is interesting to note that the United States Supreme Court has decided to adjudicate upon the *Association for Molecular Pathology et al v. Myriad Genetics Inc et al* case and its Judgement is expected to be delivered in June 2013.[198] In my opinion, the United States Supreme Court will tailor a judgement that would be fairly similar to the decision of the European Court of Justice in the case of *Monsanto Technology LLC v. Cefetra BV and Others*. Thus, it will bring the patent regimes even closer.

**117** The rationale behind the decision of the European Court of Justice is that the research and development in the field of biotechnology over a particular purified and isolated DNA sequence should not be restricted. Others should have the right to research and make academic contributions freely, without fear of patent infringement litigations.

**118** However, on the other hand, biotechnology is a field that requires high amounts of investment. If an investor cannot fully secure his interest, he or she most probably will be precluded from disclosing an invention or will not invest in the first place. Thus instead of promoting research and development in the field, this policy could actually promote stagnation.

**119** Will the United States Supreme Court rule on the issue of *purpose bound patents* versus *absolute product patents* in the same manner as the European Court of Justice did, or will it choose to follow another policy path? And which is the *right* policy to follow? Only time will answer those questions.

■

* This descriptive Research Paper was written under the supervision and helpful guidance of Mr Aurélien Lorange LL.M.

1 There is a vast amount of media coverage concerning the field of Biotechnology, e.g. Reuters, Scientists See Biotech Battle (The New York Times, 1987) http://www.nytimes.com/1987/06/23/business/scientists-see-biotech-battle.html?ref=biotechnology, accessed 6 February 2013; K. Schneider, Witnesses Clash on Animal

Patents (The New York Times, 1987) http://www.nytimes.com/1987/06/12/us/witnesses-clash-on-animal-patents.html?ref=biotechnology, accessed 6 February 2013; J. Tierney, Are Scientists Playing God? It Depends on Your Religion (The New York Times, 2007) http://www.nytimes.com/2007/11/20/science/20tier.html?pagewanted=all&_r=0, accessed 6 February 2013; J. Chatzimarkakis, Getting an appetite for biotechnology (BBC NEWS, 2009) http://news.bbc.co.uk/2/hi/science/nature/7905567.stm, accessed 6 February 2013.

2 Convention on Biological Diversity (adopted 22 May 1992, entered into force 29 December 1993) 1760 UNTS 79, Article 2.

3 For example, early civilizations such as the ones in Mesopotamia and Egypt understood and studied the importance of biotechnology in the fields of agriculture and animal husbandry; another example of early developments in biotechnology is the process of Ethanol fermentation; See W. Thieman and M. Palladino *Introduction to Biotechnology* (2nd edn, Benjamin Cummings, San Francisco 2004); J. Arnold, *Origin and History of Beer and Brewing: From Prehistoric Times to the Beginning of Brewing Science and Technology* (Alumni Association of the Wahl-Henius Institute of Fermentology, Chicago 1911).

4 D. Chisum, *Chisum on patents: a treatise on the law of patentability, validity, and infringement* (LEXIS pub, New York 1978) at 7-200.

5 See A. Gustafsson 'Patenting Human DNA Sequences Absolute Product Patents - A Reasonable Degree of Protection?' (LL.M. Thesis, University of Lund 2007).

6 V. Ling, 'Patently Ours? Constitutional Challengs to DNA Patents' (2012) 14 UPJCL 813, 848; See Universal Declaration on the Human Genome and Human Rights, UNGA Res 53/152 (10 Mar 1999) (adopted by unanimity); Parliamentary Assembly, 'Protection of the human genome by the Council of Europe' (Recommendation 1512, 2001) http://assembly.coe.int/Documents/AdoptedText/ta01/EREC1512.htm, accessed 5 February 2013; World Medical Association, 'World Medical Association Council Meeting' (press release, 2000) http://www.wma.net/en/40news/20archives/2000/2000_16/index.html, accessed 5 February 2013.

7 *Patenting Human DNA Sequences Absolute Product Patents - A Reasonable Degree of Protection?* (n 5) p. 5.

8 Directorate-General for Research and Innovation, European Commission, S. Bostyn 'Patenting DNA sequences (polynucleotides) and scope of protection in the European Union: an evaluation' (2004) KI-NA-21-122-EN-C p. 3.

9 Convention on the Grant of European Patents (European Patent Convention) (adopted 5 October 1973, entry into force 7 October 1977) 1065 UNTS 199 (EPC).

10 Patent Cooperation Treaty (adopted 19 June 1970, entered into force 24 January 1978) 1160 UNTS 231.

11 On 29th of June 2012, the Competitiveness Council of Ministers reached an agreement in relation to the adoption of a proposed Regulation for the creation of an EU-wide patent and the establishment of a Patent Court; See Academy of European Law, 'Speakers' Contributions - The Creation of Unitary Patent Protection in The European Union' Paris, 29-30 November 2012.

12 See World Health Organisation (Report of The Advisory Committee on Health Research), 'Genetics, genomics and the patenting of DNA: Review of potential implications for health in developing countries' (2005) LC/NLM classification: QU 33.1 p.15.

13 European Parliament and Council Regulation (EU) 1257/2012 of 17 December 2012, implementing enhanced cooperation in the area of the creation of unitary patent protection [2012] OJ L361 (Unitary Patent Regulation); Council Regulation (EU) 1260/2012 of 17 December 2012, implementing enhanced cooperation in the area of the creation of unitary patent protection with regards to the applicable translation arrangements [2012] OJ L361/89 (Translation Regulation).

14 Council of the European Union doc. 16351/12 of 11 January 2013, Agreement on a Unified Patent Court [2013].

15 Dr. M. Ficsor, 'Coexistence of National Patents, European Patents and Patents With Unitary Effect,' 'ERA Conference on the Creation of Unitary Patent Protection in the European Union,' Paris, 29-30 November 2012 p.11; See *Speakers' Contributions - The Creation of Unitary Patent Protection in The European Union* (n 9) p.19.

16 See *Unitary Patent Regulation* (n 13) Article 18; *Translation Regulation* (n 13) Article 7 (2).

17 See *Agreement on a Unified Patent Court* (n 14) Article 89.

18 *Genetics, genomics and the patenting of DNA: Review of potential implications for health in developing countries* (n 10) p. 15.

19 WIPO administers 25 treaties, three of those jointly with other international organizations; See World Intellectual Property Organization 'WIPO-Administered Treaties' http://www.wipo.int/treaties/en/index.jsp, accessed 3 February 2013.

20 Agreement of Trade-Related Aspects of Intellectual Property Rights, Including Trade in Counterfeit Goods (adopted 15 April 1994, entered into force 1 January 2005) 1869 UNTS 299 (TRIPS).

21 For example, in Brazil, an inventor cannot patent "the genome or germplasm of any natural living being, when found in nature or isolated therefrom, and natural biological processes," but he or she could patent a gene sequence. See Section 1, Article 10 IX of Industrial Property Law No. 9279/96; see *Genetics, genomics and the patenting of DNA: Review of potential implications for health in developing countries* (n 10) p. 76.

22 The "first-to-invent" patent system will be altered on 16th of March 2013, after the "Leahy-Smith America Invents Act" (H.R.1249 - America Invents Act to amend title 35, United States Code, to provide for patent reform), adopted under the Obama Administration. The new patent system will be "first-inventor-to-file" and is considered to bring the American patent regime close to the ones of Europe and Japan.

23 The Constitution of the United States, Article I, Section 8.

24 35 *USC* Part I.

25 35 *USC* Part II.

26 35 *USC* 101.

27 35 *USC* 102.

28 35 *USC* 101.

29 35 *USC* 103.

30 *Diamond v. Chakrabarty*, 447 U.S. 303, 313 (1980).

31 *Funk Brothers Seed Co. v. Kalo Inoculant Co*, 333 U.S. 127 (1948).

32 *Ibid* at 130.

33 See E. Gold, J. Carbone, 'Detailed legal analysis of gene patents, competition law and privacy law' in E. Gold, J. Carbone 'Myriad Genetics: In the eye of the policy storm' Appendix B (2010) 12 Genetics in Medicine 39, 70.

34 *Diamond v. Chakrabarty* (n 30).

35 Dr. P. Janicke, 'IP Survey – Patent Cases 2012' (2012), University of Houston Law Center.

36 *In re Bergy*, 563 F.2d 1031 (1977).

37 *Ibid.*

38 *Detailed legal analysis of gene patents, competition law and privacy law* (n 33).

39 USP 4,259,444, Microorganisms having multiple compatible degradative energy-generating plasmids and preparation thereof (Patent, 1981) http://patft.uspto.gov/netacgi/nph-Parser?Sect2=PTO1&Sect2=HITOFF&p=1&u=/netahtml/PTO/search-bool.html&r=1&f=G&l=50&d=PALL&RefSrch=yes&Query=PN/4259444, accessed 6 April 2013.

**40** *Detailed legal analysis of gene patents, competition law and privacy law* (n 33).

**41** Organisation for Economic and Cooperative Development, 'Genetic Inventions, Intellectual Property Rights and Licensing Practices: Evidence and Policies' (OECD Publications, Paris 2002).

**42** R. Singh, Dr. L. Walters, 'DNA Patent Database,' Kennedy Institute of Ethics (Georgetown University, Washington DC 2009).

**43** K. Jensen and F. Murray, "Intellectual Property Landscape of the Human Genome" (2005) 310 Science 239.

**44** *Detailed legal analysis of gene patents, competition law and privacy law* (n 33).

**45** E. Rogers, 'Can You Patent Genes? Yes and No' (2011) 93 JPTOS 19, 19.

**46** *Association for Molecular Pathology v. Myriad Genetics*, 653 F.3d 1329, 1358 (2012).

**47** See S. Merrill and A. Mazza, *Reaping the Benefits of Genomic and Proteomic Research: Intellectual Property Rights, Innovation, and Public Health* (1st edn, National Academy Press, Washington, DC 2006).

**48** See The Nuffield Council on Bioethics, 'The ethics of patenting DNA a discussion paper' (2002), London; Danish Council of Ethics, 'Patenting human genes and stem cells' (2004), Copenhagen.

**49** See T. Caulfield, 'Evidence and Anecdotes: An Analysis of Human Gene Patenting Controversies' (2006) 24 Nature Biotechnology 1091; G. van Overwalle and E. van Zimmeren, 'Reshaping Belgian Patent Law: The Revision of the Research Exemption and the Introduction of a Compulsory License for Public Health' (2006) 64 Chizaiken Forum 42, 49; J. Warcoin, "Patent Tsunami' in the Field of Genetic Diagnostics: A Patent Practitioner's View' (2009) 331, 338 in G. van Overwalle, *Gene Patents and Collaborative Licensing Models Patent Pools, Clearinghouses, Open Source Models and Liability Regimes* (CUP, Cambridge 2009).

**50** See, *Patently Ours? Constitutional Challenges to DNA Patents* (n 6) p. 823.

**51** USP 5,747,282, 17Q-linked breast and ovarian cancer susceptibility gene (Patent, 1998) http://patft.uspto.gov/netacgi/nph-Parser?Sect2=PTO1&Sect2=HITOFF&p=1&u=/netahtml/PTO/search-bool.html&r=1&f=G&l=50&d=PALL&RefSrch=yes&Query=PN/5747282, accessed 6 February 2013;

USP 5,837,492, Chromosome 13-linked breast cancer susceptibility gene (Patent, 1998) http://patft.uspto.gov/netacgi/nph-Parser?Sect2=PTO1&Sect2=HITOFF&p=1&u=/netahtml/PTO/search-bool.html&r=1&f=G&l=50&d=PALL&RefSrch=yes&Query=PN/5837492, accessed 6 February 2013;

USP 5,693,473, Linked breast and ovarian cancer susceptibility gene (Patent, 1997) http://patft.uspto.gov/netacgi/nph-Parser?Sect2=PTO1&Sect2=HITOFF&p=1&u=/netahtml/PTO/search-bool.html&r=1&f=G&l=50&d=PALL&RefSrch=yes&Query=PN/5693473, accessed 6 February 2013;

USP 5,709,999, Linked breast and ovarian cancer susceptibility gene (Patent, 1998) http://patft.uspto.gov/netacgi/nph-Parser?Sect2=PTO1&Sect2=HITOFF&p=1&u=/netahtml/PTO/search-bool.html&r=1&f=G&l=50&d=PALL&RefSrch=yes&Query=PN/5709999, accessed 6 February 2013;

USP 5,710,001, 17q-linked breast and ovarian cancer susceptibility gene, (Patent, 1998) http://patft.uspto.gov/netacgi/nph-Parser?Sect2=PTO1&Sect2=HITOFF&p=1&u=/netahtml/PTO/search-bool.html&r=1&f=G&l=50&d=PALL&RefSrch=yes&Query=PN/5710001, accessed 6 February 2013;

USP 5,753,441, 170-linked breast and ovarian cancer susceptibility gene, (Patent, 1998) http://patft.uspto.gov/netacgi/nph-Parser?Sect2=PTO1&Sect2=HITOFF&p=1&u=/netahtml/PTO/search-bool.html&r=1&f=G&l=50&d=PALL&RefSrch=yes&Query=PN/5753441>, accessed 6 February 2013;

USP 6,033,857, Chromosome 13-linked breast cancer susceptibility gene (Patent, 2000) http://patft.uspto.gov/netacgi/nph-Parser?Sect2=PTO1&Sect2=HITOFF&p=1&u=/netahtml/PTO/search-bool.html&r=1&f=G&l=50&d=PALL&RefSrch=yes&Query=PN/6033857, accessed 6 February 2013.

**52** *Association for Molecular Pathology v. Myriad Genetics* (n 46) at 1339; *Patently Ours? Constitutional Challenges to DNA Patents* (n 6) p. 824.

**53** N. Howlader, A. Noone, M. Krapcho, N. Neyman, R. Aminou, S. Altekruse, C. Kosary, J. Ruhl, Z. Tatalovich, H. Cho, A. Mariotto, M. Eisner, D. Lewis, H. Chen, E. Feuer, K. Cronin, 'SEER Cancer Statistics Review, 1975-2008,' (National Cancer Institute 2010) http://seer.cancer.gov/csr/1975_2008/results_merged/, accessed 6 February 2013; see *Association for Molecular Pathology v. Myriad Genetics* (n 46) at 1339; see, *Patently Ours? Constitutional Challenges to DNA Patents* (n 6) p. 814.

**54** *Association for Molecular Pathology v. Myriad Genetics* (n 46) at 1339; see American Cancer Society, 'Breast Cancer' (description of the BRCA1 and BRCA2 genes as major reason for development of breast cancer) http://www.cancer.org/cancer/breastcancer/detailedguide/breast-cancer-risk-factors, accessed 6 February 2013; see, *Patently Ours? Constitutional Challenges to DNA Patents* (n 6) p. 815.

**55** *Patently Ours? Constitutional Challenges to DNA Patents* (n 6) p. 815.

**56** *Association for Molecular Pathology v. Myriad Genetics* (n 46) at 1340.

**57** *Association for Molecular Pathology v. Myriad Genetics* (n 46) at 1341.

**58** *Patently Ours? Constitutional Challenges to DNA Patents* (n 6) p. 828.

**59** For detailed and structured analysis on the issue see *Patently Ours? Constitutional Challenges to DNA Patents* (n 6).

**60** *Association for Molecular Pathology v. Myriad Genetics* (n 46) at 1351; *Patently Ours? Constitutional Challenges to DNA Patents* (n 6) p. 815.

**61** *Association for Molecular Pathology v. Myriad Genetics* (n 46) at 1351; *Patently Ours? Constitutional Challenges to DNA Patents* (n 6) p. 827.

**62** *Association for Molecular Pathology v. Myriad Genetics* (n 46) at 1355-1357.

**63** *Association for Molecular Pathology v. Myriad Genetics* (n 46) at 1358; *Patently Ours? Constitutional Challenges to DNA Patents* (n 6) p. 826.

**64** *Association for Molecular Pathology et al v. Myriad Genetics Inc. et al*, Docket No. 12-398, United States Supreme Court.

**65** *Mayo Collaborative Services v. Prometheus Laboratories, Inc*. 566 U. S. ____ (2012).

**66** USP 6,355,623, Method of treating IBD/Crohn's disease and related conditions wherein drug metabolite levels in host blood cells determine subsequent dosage (Patent, 2002) http://patft.uspto.gov/netacgi/nph-Parser?Sect2=PTO1&Sect2=HITOFF&p=1&u=/netahtml/PTO/search-bool.html&r=1&f=G&l=50&d=PALL&RefSrch=yes&Query=PN/6355623, accessed 21 February 2013. USP 6,680,302, Methods of optimizing drug therapeutic efficacy for treatment of immune-

mediated gastrointestinal disorders (Patent, 2004) http://patft.uspto.gov/netacgi/nph-Parser?Sect2=PTO1&Sect2=HITOFF&p=1&u=/netahtml/PTO/search-bool.html&r=1&f=G&l=50&d=PALL&RefSrch=yes&Query=PN/6680302, accessed 21 February 2013.

**67** J. Thomas, 'Mayo v. Prometheus: Implications for Patents, Biotechnology, and Personalized Medicine' (2012) 7-5700 CRS Report for Congress R42815.

**68** P. Jackman and L. Brandes, 'Mayo Collaborative Services v. Prometheus Labs., Inc.: Medical diagnostic methods merely applying a law of nature are not eligible for patent protection' (Sterne, Kessler, Goldstein & Fox, MSBA Annual IP Law Update 2012) http://www.skgf.com/media/pnc/4/media.1734.pdf, accessed 25 February 2013.

**69** *Mayo v. Prometheus: Implications for Patents, Biotechnology, and Personalized Medicine* (n 67) p. 7.

**70** "The classic test of patent-eligibility of method claims is the *machine-or-transformation test*, which grants patent-eligibility to a process claim if it (1) is implemented with a particular machine specifically devised and adapted to carry out the process in a way that is not concededly conventional nor trivial; or else (2) transforms an article from one thing or state to another."; see R. Xu, 'From Prometheus to Myriad to Classen, What a Messy Subject Matter: A Review on Recent Life Science Method Patent Cases' (2013) 11 NJTIP 119, 138; *Bilski v. Kappos,* 561 U.S. ___ , 130 S. Ct. 3218 (2010).

**71** *Mayo v. Prometheus: Implications for Patents, Biotechnology, and Personalized Medicine* (n 67) p. 6.

**72** *Prometheus Labs, Inc. v. Mayo Collaborative Services*, 628 F.3d 1347, 1355 (2010).

**73** *Mayo Collaborative Services v. Prometheus Laboratories, Inc.* (n 65) p. 2.

**74** *Mayo v. Prometheus: Implications for Patents, Biotechnology, and Personalized Medicine* (n 67) p. 7.

**75** *Parker v. Flook*, 437 U. S. 591 (1978).

**76** *Diamond v. Diehr*, 450 U.S. 175, 187 (1981).

**77** *Mayo Collaborative Services v. Prometheus Laboratories, Inc.* (n 65) p. 8.

**78** See *Ibid* p. 9.

**79** *Mayo v. Prometheus: Implications for Patents, Biotechnology, and Personalized Medicine* (n 67) p. 8.

**80** *Diamond v. Diehr* (n 76) at 191-192.

**81** *Bilski v. Kappos* (n 70) at 14.

**82** *USP 6,355,623* (n 66) col. 9, ll. 12–65, 2 App. 11; col. 8, ll. 37–40, id. at 10.

**83** *Mayo Collaborative Services v. Prometheus Laboratories, Inc.* (n 65) p. 10.

**84** *Mayo Collaborative Services v. Prometheus Laboratories, Inc.* (n 65) p. 9.

**85** *Mayo v. Prometheus: Implications for Patents, Biotechnology, and Personalized Medicine* (n 67) p. 8; See *Mayo Collaborative Services v. Prometheus Laboratories, Inc.* (n 65) p. 9.

**86** See *Mayo Collaborative Services v. Prometheus Laboratories, Inc.* (n 65) p. 11.

**87** *Ibid.*

**88** *Diamond v. Diehr* (n 76).

**89** *Parker v. Flook* (n 75).

**90** *Mayo Collaborative Services v. Prometheus Laboratories, Inc.* (n 65) p. 13.

**91** *Mayo Collaborative Services v. Prometheus Labs, Inc.: Medical diagnostic methods merely applying a law of nature are not eligible for patent protection* (n 68) p. 5.

**92** *Mayo Collaborative Services v. Prometheus Laboratories, Inc.* (n 65) p. 20.

**93** See *Mayo Collaborative Services v. Prometheus Laboratories, Inc.* (n 65) p. 21.

**94** See *Mayo Collaborative Services v. Prometheus Laboratories, Inc.* (n 65) p. 22.

**95** See *Mayo Collaborative Services v. Prometheus Laboratories, Inc.* (n 65) pp. 23-24; *Mayo v. Prometheus: Implications for Patents, Biotechnology, and Personalized Medicine* (n 67) p. 9.

**96** A. Jauhar and S. Narnaulia, 'Patenting Life the American, European and Indian Way' (2010) 15 JIPR 55, 57.

**97** *EPC* (n 9).

**98** Parliament and Council Directive (EC) 98/44 of 6 July 1998 on the legal protection of biotechnological inventions [1998] OJ L213 (Biotech Directive).

**99** See European Patent Organisation 'Member states of the European Patent Organisation' (contracting states) http://www.epo.org/about-us/organisation/member-states.html, accessed 07 December 2012.

**100** Treaty on the Functioning of the European Union [2010] OJ C83/47 Article 288.

**101** A. Tombling, J. Wilson, 'Divergent Practices across Europe for Biotechnology Patents - The Biotech Directive' (World Patent & Trademark News, 2007) http://www.wptn.com/Mailing/Feb_2007_4/details/patents/divergent.html, accessed 3 February 2013.

**102** C-377/98 *Kingdom of the Netherlands v. European Parliament and Council of the European Union* [2001] ECR I- 07079.

**103** Inserted by decision of the Administrative Council of 16.06.1999, which entered into force on 9 January 1999 (OJ EPO 1999, 437 ff) Implementing Regulations to the Convention on the Grant of European Patents (adopted 5 October 1973, as last amended 9 December 2004) Part II, Chapter VI Rule 23(b)-(e) (EPC 2000 Rule 28(b)-(e)).

**104** E.g. Implementing Regulations to the Convention on the Grant of European Patents (adopted 5 October 1973, as last amended 9 December 2004) Part II, Chapter VI, Rule 23(d) (EPC 2000 Rule 28(d)) - prohibiting the patentability of processes for cloning human beings.

**105** *EPC* (n 9) Article 52.

**106** *EPC* (n 9) Article 53.

**107** *EPC* (n 9) Article 52(1), in conjunction with *EPC* (n 9) Article 56 first sentence.

**108** *EPC* (n 9) Article 57, with the exception provided by *EPC* (n 9) Article 52 (4).

**109** *Patenting Life the American, European and Indian Way* (n 96) p. 57.

**110** T 0356/93 *Plant cells resistant to glutamine synthetase inhibitors, made by genetic engineering*/PLANT GENETIC SYSTEMS (1995) EPOR 357.

**111** *Plant cells resistant to glutamine synthetase inhibitors, made by genetic engineering* (n 110) para. 5.

**112** *Plant cells resistant to glutamine synthetase inhibitors, made by genetic engineering* (n 110) para. 6.

**113** T 0272/95 *Molecular cloning and characterization of a further gene sequence coding for human relaxin/* HOWARD FLOREY INSTITUTE OF EXPERIMENTAL PHYSIOLOGY AND MEDICINE (2002) EPOR 541.

**114** T 0019/90 *Onco-mouse*/HARVARD (1990) EPOR 501.

**115** *Hromone Relaxin*/HOWARD FLOREY INSTITUTE (n 113).

**116** W. Cornish, D. Llewelyn and T. Aplin, *Intellectual Property: Patents, Copyright, Trade Marks and Allied Rights* (7th edn, Sweet & Maxwell, London 2010) pp. 930-931.

**117** T 0315/03 *Transgenic animals*/HARVARD (2004) OJ EPO 15, 78 (TBA).

**118** *Onco-mouse* (n 114) EPOR 501.

**119** *Onco-mouse* (n 114) EPOR 525.

**120** L. Bently and B. Sherman, *Intellectual Property Law* (3rd edn, OUP, Oxford 2009) p. 442.

**121** *Onco-mouse* (n 114) EPOR 513.

**122** *Ibid.*

**123** *Ibid.*

**124** See *Onco-mouse* (n 114) EPOR 527.

**125** E. O'Sullivan, 'Article 53(a) EPC and the patentability of animals: The effect of Rule 23d(d) on *ordre public* and morality evaluations in the European Patent Office' (International Association for the Advancement of Teaching and Research in Intellectual Property, Essay 2008).

**126** *Intellectual Property: Patents, Copyright, Trade Marks and Allied Rights* (n 116) p. 929.

**127** C-428/08 *Monsanto Technology LLC v Cefetra BV and Others* [2010] ECR I-06765.

**128** EP 0 546 090, Glyphosate tolerant 5-enolpyruvylshikimate-3-phosphate synthases (Patent, 1996) https://data.epo.org/publication-server/getpdf.jsp?pn=0546090&ki=B2&cc=EP, accessed 7 February 2013.

**129** One of the most common herbicides is Glyphosate.

**130** *Monsanto Technology LLC v. Cefetra BV and Others* (n 127) para. 33.

**131** For an analysis of the term "absolute product protection" see Part E, 2, (1) of this Research Paper.

**132** *Monsanto Technology LLC v. Cefetra BV and Others* (n 127) para. 38.

**133** *Monsanto Technology LLC v. Cefetra BV and Others* (n 127) paras. 41-42.

**134** *Monsanto Technology LLC v. Cefetra BV and Others* (n 127) para. 46.

**135** *Monsanto Technology LLC v. Cefetra BV and Others* (n 127) para. 51.

**136** *Monsanto Technology LLC v. Cefetra BV and Others* (n 127) para. 58.

**137** European Commission Legal Service, C-428/08 Monsanto Technology LLC, judgment of 6 July 2010 (summaries of important cases, 2010) http://ec.europa.eu/dgs/legal_service/arrets/08c428_en.pdf, accessed 7 February 2013.

**138** *Monsanto Technology LLC v. Cefetra BV and Others* (n 127) para. 64.

**139** *Monsanto Technology LLC v. Cefetra BV and Others* (n 127) para. 69.

**140** *TRIPS* (n 20) Article 27; *TRIPS* (n 20) Article 30.

**141** *Monsanto Technology LLC v. Cefetra BV and Others* (n 127) para. 70.

**142** Joined Cases C-300/98 and C-392/98 *Dior and Others* [2000] ECR I-11307.

**143** *Monsanto Technology LLC v. Cefetra BV and Others* (n 127) para. 74.

**144** *Monsanto Technology LLC v. Cefetra BV and Others* (n 127) para. 77.

**145** *Intellectual Property: Patents, Copyright, Trade Marks and Allied Rights* (n 116) p. 231; see *Reynolds v. Smith* 20 RPC 123 (1913) at 126; see G. Kolle, 'The Patentable Invention in the European Patent Convention' (1974) 5 IIC 140 at 147-148.

**146** See *Diamond v. Diehr* (n 80).

**147** *Mayo Collaborative Services v. Prometheus Laboratories, Inc.* (n 65).

**148** *Biotech Directive* (n 98) Article 5 (1).

**149** *Biotech Directive* (n 98) Article 5 (2).

**150** *The ethics of patenting DNA a discussion paper* (n 48) p. 23.

**151** 'Trilateral Co-operation of the US, European and Japanese Patent Offices' (1988) 7 Biotechnology Law Review 159, 163.

**152** R. Crespi, 'PATENTS ON GENES - do they have a future ?' (2006) p. 2 http://www.law.ed.ac.uk/ahrc/files/81_crespipatentsongenes00.pdf, accessed 4 February 2013.

**153** *Patenting DNA sequences (polynucleotides) and scope of protection in the European Union: an evaluation* (n 8) pp. 17, 44; *Biotech Directive* (n 98).

**154** T 0301/87 *Alpha-interferons/BIOGEN* (1990) EPOR 190.

**155** H. Jaenichen, L. McDonell and J. Haley, *From Clones to Claims* (Carl Heymanns Verlag, Cologne 2002) 420-421; see *Hromone Relaxin*/HOWARD FLOREY INSTITUTE (n 113).

**156** *Patenting DNA sequences (polynucleotides) and scope of protection in the European Union: an evaluation* (n 8) p. 45.

**157** *Patenting DNA sequences (polynucleotides) and scope of protection in the European Union: an evaluation* (n 8) p. 46.

**158** *The ethics of patenting DNA a discussion paper* (n 48) p. 29.

**159** *Intellectual Property Law* (n 120) p. 493; see *Technograph Printed Circuits v. Mills & Rockley* [1972] RPC 346, 355; see T 0038/93 *Allied colloids*/POLYMER POWDERS (1997) OJ EPO 134, 149.

**160** See T 0060/89 *Fusion Proteins*/HARVARD (1990) OJ EPO 268 at 2.2.4.

**161** *In Re Deuell,* 51 F.3d 1552, 1559 (1995).

**162** 35 *USC* 103(a), "Patentability shall not be negative by the manner in which the invention was made."

**163** *The ethics of patenting DNA a discussion paper* (n 48) p. 29.

**164** Observing software simulations without actually performing the operation in question.

**165** *In Re Deuell* (n 161).

**166** See *From Clones to Claims* (n 155) p. 509.

**167** See *From Clones to Claims* (n 155) p. 510-515; see A. Nelson, 'Obviousness or Inventive Step as Applied to Nucleic Acid Molecules: A Global Perspective' (2004) 6 NCJLT 1, 40.

**168** European Patent Office, Japan Patent Office and United States Patent and Trademark Office, 'Trilateral Project B3b: Mutual Understanding in Search and Examination,' in Annex 2 'Report on Comparative Study on Biotechnology Patent Practices' (2001).

**169** This was confirmed in a judgment by the English Court of Appeal, see *Chiron Corporation and Others v. Murex Diagnostics Ltd. and Others* (1996) RPC 535.

**170** Standing Committee on the Law of Patents, '"Industrial Applicability" and "Utility" Requirements: Commonalities and Differences', Ninth Session (2003).

**171** *Ibid* p.2.

**172** *Biotech Directive* (n 98) Article 5(3).

**173** *Biotech Directive* (n 98) Recital 23.

**174** Department of Commerce Patent and Trademark Office, 'Utility Examination Guidelines' (950706172-5172-01, 1995).

**175** *Ibid.*

**176** *The ethics of patenting DNA a discussion paper* (n 48) p. 31.

**177** See *Patenting DNA sequences (polynucleotides) and scope of protection in the European Union: an evaluation* (n 8) p. 51; J. Conley, Roberte Makowski, 'Back to the Future: Rethinking the Product of Nature Doctrine as a Barrier to Biotechnology Patents' (2003) 85 JPTOS 301, 11.

**178** T 0870/04 *BDP1 Phosphatase*/MAX-PLANCK (2005) (Not Reported) at point 21 of the reasons.

**179** *The ethics of patenting DNA a discussion paper* (n 48) p. 31.

**180** *Patenting DNA sequences (polynucleotides) and scope of protection in the European Union: an evaluation* (n 8) p. 105.

**181** *Patenting DNA sequences (polynucleotides) and scope of protection in the European Union: an evaluation* (n 8) p. 107.

**182** *Patenting DNA sequences (polynucleotides) and scope of protection in the European Union: an evaluation* (n 8) p.108.

**183** *Patenting DNA sequences (polynucleotides) and scope of protection in the European Union: an evaluation* (n 8) p.108.

**184** "For a detailed analysis of the issues relating to the patentability of genetically manipulated animals and plants and the scope of protection of such inventions, see, S. Bostyn, 'The Patentability of Genetic Information Carriers; The New E.U. Directive 98/44/EC on the Legal Protection

of Biotechnological Inventions' (1999) IPQ 13-26.; G 0001/98 *Transgenic plant*/NOVARTIS II (1999) EPOR 303.; See C-377/98 *Kingdom of the Netherlands v European Parliament and Council of the European Union* [2001] ECR I- 07079 paras. 42-49.; Opinion of Advocate General Jacobs in case C-377/98 *Kingdom of the Netherlands v European Parliament and Council of the European Union* [2001] ECR I- 07079, delivered on 14 June 2001 paras. 113-141"; *Patenting DNA sequences (polynucleotides) and scope of protection in the European Union: an evaluation* (n 8) p.108.

**185** "The term composition of matter patent is sometimes used in the United States to refer to a patent on a chemical product. Confusingly, it has been used in relation to both individual substances and true compositions of two or more substances." See *The ethics of patenting DNA a discussion paper* (n 48) p. 25.

**186** *The ethics of patenting DNA a discussion paper* (n 48) p. 24.

**187** *The ethics of patenting DNA a discussion paper* (n 48) p. 25.

**188** Specified in the patent application.

**189** *Patenting Human DNA Sequences Absolute Product Patents - A Reasonable Degree of Protection?* (n 5) p.36; See S. Bostyn, 'Protection of biotechnological inventions in France and Germany after directive 98/44/EC,' 欧州知的財産ニュース (2005 年 5月号) available at http://www.jetro.go.jp/world/europe/ip/archive/pdf/news_009_1.pdf, accessed 8 February 2013.

**190** And successfully registered.

**191** *Patenting Human DNA Sequences Absolute Product Patents - A Reasonable Degree of Protection?* (n 5) p. 33.

**192** USP 2,507,193, Penicillin Product (Patent, 1950) http://www.google.com/patents?id=bExkAAAAEBAJ&printsec=abstract&zoom=4#v=onepage&q&f=false, accessed 3 February 2013; See *Patenting Human DNA Sequences Absolute Product Patents - A Reasonable Degree of Protection?* (n 5) p. 33.

**193** *Association for Molecular Pathology v. Myriad Genetics* (n 46).

**194** *Monsanto Technology LLC v. Cefetra BV and Others* (n 127).

**195** G0002/88 *Friction reducing additive*/MOBIL OIL III (1989) OJ EPO 93 at p. 15.

**196** *Patenting Human DNA Sequences Absolute Product Patents - A Reasonable Degree of Protection?* (n 5) p. 36.

**197** In the face of the European Union.

**198** *Association for Molecular Pathology et al v. Myriad Genetics Inc et al* Docket No. 12-398, United States Supreme Court http://www.supremecourt.gov/Search.aspx?FileName=/docketfiles/12-398.htm accessed 6 April 2013.

# Swiss Patent Jurisprudence 2012

by **Cyrill P. Rigamonti***
Dr. iur. (Zurich), LL.M. (Georgetown), S.J.D. (Harvard), Professor of Law and Chair, Department of Economic Law, University of Bern, Switzerland

**Abstract:** The new Swiss Federal Patent Court, with nationwide first-instance jurisdiction over all civil patent matters, has been operating since 1 January 2012. This article reviews and contextualizes the most important patent cases published in 2012 by the Swiss Federal Patent Court and the Swiss Federal Supreme Court. It concludes that the revamped Swiss patent litigation system has the potential of turning Switzerland into a competitive venue for the adjudication of patent matters in Europe.

**Keywords:** Intellectual Property, Patents, Litigation, Switzerland, Patent Court, Specialized Courts, Specialized Judges, Technical Judges, Expert Opinions, Preliminary Injunctions, Provisional Measures, Civil Procedure, Infringement, Novelty, Inventive Step, Non-obviousness, Requests for Relief, Pre-Trial Taking of Evidence, Precise Description



Recommended citation: Cyrill P. Rigamonti, Swiss Patent Jurisprudence 2012, 4 (2013) JIPITEC 53, para. 1.

## A. Introduction

1 The year 2012 marked the beginning of a completely new era in Swiss patent litigation. The newly created Swiss Federal Patent Court, a first-instance trial court with nationwide jurisdiction over all civil patent matters, began operating on 1 January 2012, and the procedural rules applicable to patent litigation were also revamped as a result of the enactment of the new Swiss Federal Code of Civil Procedure in 2011.[1] The primary goal behind these institutional and procedural changes was to professionalize the adjudication of patent cases and to ensure quick and cost-effective proceedings on the trial level, in part to make Switzerland a more attractive venue for international patent litigants and litigators.[2]

2 The concentration of patent cases in the hands of a single court with nationwide jurisdiction was only one element of the strategy adopted by the Swiss legislature. An equally important element was the substitution of court-appointed technical experts with a large number of technically trained adjunct judges,[3] because the routine use of external experts was a major source of delay and costs under the old system.[4] By contrast, relying on part-time technical judges who are paid on a case-by-case basis not only tends to reduce costs, but also shortens the proceedings significantly, mostly because the selection and instruction of a technical judge is an internal matter and because there are virtually no procedural devices allowing the parties to influence or formally suggest amendments to the subject matter of the technical judge's report or statement.[5] Accordingly, the Swiss Federal Patent Court's policy is to always rely on technical judges rather than court-appointed experts, unless extensive testing is required or the technical field in question is so peculiar that there is no technical judge on the court with the appropriate expertise. So far, the Swiss Federal Patent Court has not appointed external experts and has relied exclusively on technical judges.[6]

3 The importance of reports or statements by technical judges cannot be underestimated.[7] While they are meant to replace reports from court-appointed experts, the subject matter of their reports or statements is not limited to factual issues, but may and typically does include legal conclusions and determinations, precisely because their role is not that of expert, but rather judge. Therefore, a party

faced with a negative statement by a technical judge cannot rebut that statement by submitting a party expert opinion or by requesting that the court appoint an expert to obtain a second opinion. Instead, if the rest of the panel adopts the factual findings and legal opinions of the technical judge, the only way to challenge the substance of the technical judge's work is to appeal the court's final decision to the Swiss Supreme Court. However, it is unlikely that the Swiss Supreme Court will disagree with a technical judge on a technical issue, given that the Supreme Court justices lack technical expertise and no experts can be brought in on appeal.

4 Regarding the duration of the proceedings,[8] the Swiss Federal Patent Court strives to complete proceedings on the merits within twelve months, but there is no reliable actual data yet, because most of the cases decided so far were inherited from the cantonal courts that had jurisdiction before 2012 (some of which stalled proceedings pending the creation of the new court, foreseeing a transfer of venue). It is unclear how long these proceedings would have taken had they initially been filed directly with the Swiss Federal Patent Court. In reality, the goal of twelve months appears to be difficult to achieve, in part because – as expected[9] – the need to accommodate the extra-judicial work schedules of part-time judges does not necessarily facilitate fast decision-making. An average of eighteen months seems more realistic, as long as the court can work without the appointment of external experts. Since the Swiss Supreme Court decides appeals within approximately six months,[10] the overall duration of patent litigation on the merits up to a final decision (on both infringement and validity)[11] should not exceed two years, which is rather short in comparison to most other European venues. Moreover, regarding summary proceedings, including those relating to preliminary injunctions, the court also appears to be on track, because it has completed all proceedings filed directly with the court within six months or less.

5 In 2012, the Swiss Federal Patent Court published nineteen decisions, the most important of which will be reviewed below.[12] It should be noted at the outset that this number is significantly lower than the number of cases actually filed,[13] because there is a relatively high rate of settlement. This is no coincidence, because the Swiss Federal Patent Court, following the example of some cantonal commercial courts, has adopted procedural guidelines that aim to enable and facilitate settlements early on.[14] After the first briefs have been exchanged, the court typically invites the parties to a court hearing ("preparatory hearing"), which consists of a formal and an informal part. During the formal part, which is transcribed, the court essentially discusses the subject matter of the case with the parties, points out where more evidentiary support is necessary, asks for clarifications should the briefs be unclear, and may take evidence. During the informal part, which is not transcribed and is strictly off the record,[15] the court gives its preliminary assessment of the case, reveals weaknesses in the parties' arguments, and tries to get the parties to settle, with considerable success. Approximately fifty percent of the cases are settled during such hearings.

6 The Supreme Court has reviewed only two Federal Patent Court decisions so far. The first case was a clear affirmation of an equally clear dismissal on procedural grounds,[16] and the second case was a partial reversal on a peculiar issue of subject matter jurisdiction.[17] The Swiss Supreme Court also published two other patent decisions in 2012, both of which had been appealed in 2011 under the old system, that is, prior to the existence of the Swiss Federal Patent Court. These cases will be included in the following review.

## B. Case Law

7 A review of the nineteen decisions published by the Swiss Federal Patent Court in 2012 reveals a certain prevalence of procedural issues, which is not surprising given the fact that the court still has to fine-tune some of its procedures on the basis of the new Swiss Code of Civil Procedure and the special procedural provisions contained in the Act on the Federal Patent Court and the Patent Act. Overall, the court is doing a good job of elaborating and communicating its practices that will form the basis of future proceedings. At the same time, the court has had the opportunity to decide a few cases involving substantive issues, which demonstrate the use and significance of reports by technical judges and the importance of the practices and case law of the European Patent Office.

## I. Procedural Issues

8 While the Swiss Federal Patent Court has had a flurry of minor procedural issues to decide,[18] there are six 2012 decisions that are particularly important. They relate (i) to the formal requirements and the admissible content of requests for relief in preliminary patent proceedings, (ii) to the new procedural devices for the pre-trial taking of evidence, and (iii) to the evidentiary status of expert opinions. On the issue of pre-trial evidence, there is also a Supreme Court case to be considered.

### 1. Requests for Relief

9 Swiss courts are fairly strict in terms of what they require in order for a request for injunctive relief

to be sufficiently determinate to be admissible. The leading Supreme Court case on the issue was decided in 2004 and held that a request for injunctive relief in patent matters is only sufficiently determinate if the accused device is described therein as a "real technical act", so that "no interpretation of legally or ambiguous technical terms is necessary",[19] because "only if the concrete technical features of the accused device that make use of the patent in litigation are spelled out, can a potential injunction be enforced".[20] The basic idea is that officials enforcing injunctions should not have to assume the role of the judge, and therefore both the order granting injunctive relief and the request for such relief must be determinate with regard to the technical features of the accused device that amount to patent infringement. Accordingly, drafting a request for injunctive relief requires both skill on behalf of the drafting attorney and sufficient information about the accused device that enables the drafting attorney to be specific in the request. It is no surprise that patent litigators wanted to have clarity about the extent to which the Swiss Federal Patent Court would follow the Supreme Court in this regard.

**10** In one of its first decisions, the Swiss Federal Patent Court made it clear that it would closely follow the Supreme Court's decision when it held that it was not sufficient to describe the accused device by simply referring to an exhibit consisting of advertising materials containing a product description, if the concrete technical features of the accused device that allegedly constituted patent infringement could not be ascertained on the basis of these materials.[21] According to the court, one must proceed in two steps, namely (i) analyze the relevant patent claim and break it down into its individual technical elements and (ii) show how every single technical element of the relevant claim is implemented in the accused device.[22] If the request for injunctive relief does not comply with these requirements, the request will be dismissed without prejudice on procedural grounds.

**11** In line with these considerations, the Swiss Federal Patent Court also dismissed without prejudice a request for a preliminary injunction in another case, because the plaintiff had simply incorporated the language of the allegedly infringed patent claim without detailing which of the technical elements in the accused device would amount to patent infringement. The court explained that while the official enforcing an injunction may well have to consult with a technical expert if faced with factual issues that the official cannot master alone, no official shall have to answer the question of whether certain facts constitute patent infringement, but instead shall simply determine whether these facts match the precise technical description in the injunction. Therefore, the request for injunctive relief must contain sufficient information about which technical elements of the accused device the plaintiff considers to be a practice of the patented invention.[23]

**12** The court's purist approach to the drafting of requests for injunctive relief is not likely to be met with great enthusiasm by practitioners, because it is seen as an unnecessarily formalist hurdle, given that the parties involved often know precisely what kind of behavior is targeted by the request for injunctive relief in question and because injunctions are often enforced autonomously by the parties without the intervention of any official.[24] Nevertheless, as a matter of principle, the court's approach merits support, because holding the parties to a high standard when drafting requests for injunctive relief facilitates the work of the court and therefore contributes to the streamlining of the proceedings. Breaking down the accused device into its technical elements and matching them with the individual technical elements in the allegedly infringed patent claim also helps to clarify the technical issues at stake and to focus the proceedings on the few technical elements that are in dispute. To the extent that it is difficult or even impossible to precisely describe the accused device for lack of information prior to the filing of the request for injunctive relief,[25] the newly available procedural remedy of precise description[26] should help (for more detail, see also *infra* para. 17). In any event, the Swiss Federal Patent Court, in the two cases summarized above, has given practitioners useful and precise guidelines regarding the proper drafting of requests for injunctive relief.

**13** Aside from requests for injunctive relief, the Swiss Federal Patent Court also had to decide whether a request for declaratory judgment regarding the ownership of a European patent was admissible as a preliminary measure in summary proceedings. Invoking the majority view expressed in scholarly writings, the court dismissed the request, finding it to be inadmissible under the general rules of civil procedure.[27] Essentially, the court reasoned that a preliminary declaration of patent ownership pending the outcome of the merit proceedings would be tantamount to a permanent order, the effect of which would and could not be limited in time. In this particular case, the court also expressed concern that the plaintiff had shown neither any legally protected interest in a court declaration of ownership nor a likelihood of irreparable harm should the preliminary declaration not be made.[28] By contrast, the court found it procedurally admissible to request that the defendant be preliminarily enjoined from alleging towards third parties that the plaintiff is not the legal owner of the patent in question.[29] Following a substantive analysis, however, the Swiss Federal Patent Court denied this request for injunctive relief, because the plaintiff had not shown the likelihood of any contractual violation or the infringement of any legal rights.[30]

## 2. Pre-Trial Taking of Evidence

**14** In view of the costs and uncertainties associated with patent litigation, it is important to have somewhat reliable information, especially about the technical features of a potentially infringing device, prior to initiating a lawsuit. To this end, there are two partially new procedural devices available to plaintiffs that allow them to better assess their evidentiary basis and the risks of litigation.[31] The first device generally enables the pre-trial taking of evidence to safeguard legitimate interests on the basis of the new Swiss Code of Civil Procedure,[32] and the second device is specific to patents in that it allows for a provisional measure that consists of the precise description of an allegedly infringing structure or process by a member of the Swiss Federal Patent Court.[33] It is no surprise that both the Swiss Supreme Court and the Swiss Federal Patent Court have already had the opportunity to express their views on these procedural novelties.

**15** In a case decided in January 2012, the Swiss Supreme Court had to review the denial of a request for the pre-trial taking of evidence to safeguard legitimate reasons in the context of a claim based on indirect patent infringement.[34] The plaintiff had asked the lower court, the Commercial Court of the Canton of Aargau, to inspect and document the facilities of a waste incineration plant in order to assess the chances of success of a patent infringement action to be brought against a defendant which had delivered component parts to the company running the waste incineration plant. It is unclear why the plaintiff did not bring the case against the waste incineration company as an alleged direct infringer, but instead filed the action against the supplier as an alleged indirect infringer. In any event, the commercial court denied the request, citing the plaintiff's failure to establish the likely existence of an act of indirect infringement committed by the defendant. The plaintiff appealed, and the Swiss Supreme Court affirmed.[35] In terms of substance, the Court took the opportunity to explain that the general device for the pre-trial taking of evidence and the patent-specific device of precise description are two different procedural avenues, and that it is perfectly fine to ask either for a precise description under the special rules or for the inspection of a waste incineration plant in accordance with the general rules.[36] More importantly, however, the Court clarified that while it is appropriate to use the general procedural device for the purpose of ascertaining litigation prospects, the requesting party must still show the likely existence of facts, based upon which substantive law provides a claim against the defendant.[37] This requirement is only relaxed regarding facts that are meant to be proven by the evidence that is the subject matter of the evidentiary request, as it is sufficient to allege these facts in a substantiated fashion.[38] In other words, while the plaintiff did not have to show the likely existence of the direct infringement to be proven with the requested evidentiary measure, it still had to show the likely existence of facts underlying its claim for indirect infringement (other than the acts constituting direct infringement), which it had not done. The mere allegation of a legitimate interest in the pre-trial taking of evidence is not enough for an evidentiary request to be granted. In plain English, fishing expeditions are not allowed under the new regime.

**16** The Swiss Federal Patent Court first applied these general principles in the context of a pharmaceutical patent case. Using the general procedural device for the pre-trial taking of evidence, the plaintiff requested that the defendant be asked about the composition of its tablets and about the identity of the supplier of the active ingredient contained in the tablets and that the defendant turn over samples of its tablets for further lab analysis.[39] In support of its requests, the plaintiff argued that the defendant had registered its tablets as a generic version of the patented drug with the Swiss authorities prior to the lapse of the relevant patents, while these tablets contained an active ingredient that *potentially* infringed the plaintiff's patents. However, in order to establish that the active ingredient in question *actually* infringed the patent, it needed more evidence and information that only the defendant could provide, because the defendant's tablets were not yet available on the Swiss market. Consequently, the plaintiff argued that it had the prerequisite "legitimate interest" in taking the requested pre-trial evidence, namely a legitimate interest in avoiding futile litigation. While the Swiss Federal Patent Court agreed with the latter, it applied the standards set forth by the Swiss Supreme Court and ultimately denied all requests, because the plaintiff had not shown the likely existence of a right to injunctive relief.[40] First, one of the patents invoked by the plaintiff had been revoked by the European Patent Office, and while the appeal was still pending and the patent was therefore still in force, the plaintiff had not explained in what sense the revocation was legally wrong.[41] In view of these facts, the court concluded that the plaintiff had not shown the likely existence of patent infringement with regard to this patent. Second, the court reached the same conclusion with regard to the process patent invoked by the plaintiff, because the mere allegation – that the plaintiff assumed that the active ingredient contained in the defendant's tablets had been produced pursuant to the patented process – was obviously not sufficient to establish a likely existence of infringement.[42] Third, the same was also true for the patent protecting a certain composition of tablets with the relevant active ingredient, because the fact alone that the defendant's tablets contained a certain active ingredient was not

sufficient to show that all elements of the relevant patent claim were fulfilled. In sum, the Swiss Federal Patent Court concluded that the plaintiff's request was an inappropriate fishing expedition for which the new procedural device for the pre-trial taking of evidence is not available.[43] This case reiterates that while there are procedural mechanisms available to help a plaintiff obtain evidence prior to the formal initiation of patent litigation, the mere allegation of a legitimate interest in obtaining such evidence is not sufficient if the underlying claim for infringement itself is also based on mere allegations.

**17** In another case, the Swiss Federal Patent Court had to apply the new rules governing the patent-specific procedural device of *precise description* for the first time.[44] Legally, it is a provisional measure that allows a plaintiff to have an allegedly infringing device or process described by a technical judge of the Swiss Federal Patent Court in order to enable the requesting party to assess its chances of success prior to filing a patent infringement action. An important feature of this provisional measure is that it no longer requires a showing that the item to be described is likely to be unavailable at trial.[45] However, the requesting party must still show that it is likely that a legal claim based on patent law has been infringed or is about to be infringed.[46] In the case at hand, the plaintiff requested a precise description of a certain process employed by the defendant, arguing that this process is likely to infringe the plaintiff's process patent. The Swiss Federal Patent Court concluded that the plaintiff had shown the likelihood of infringement of a legal claim arising out of patent law, because the defendant was the successor to a bankrupt company that had undeniably practiced the patented invention and from which the defendant had inherited its facilities, means of production and much of its personnel.[47] The defendant's argument – that its process was practiced at temperatures other than those mentioned in the relevant patent claim – was rejected by the court, precisely because only a description of the defendant's process could establish whether this was true. Accordingly, the court ordered a precise description of the defendant's process.[48] In order to protect any business secrets, the plaintiff was not allowed to be present when the precise description was taken, but the court allowed the plaintiff's attorney and patent attorney to participate, subject to a duty of confidentiality, that is, a duty not to disclose anything perceived during the precise description to their client, the plaintiff, until the plaintiff was formally notified by the court.[49] In this respect, the Swiss Federal Patent Court adopted, without acknowledgement, the description procedure practiced by the German courts in Düsseldorf.[50] What is important about this case is that it demonstrates that it is possible for a plaintiff to meet the burden of showing a likelihood of infringement in order to obtain a pre-trial precise description. It also shows how the court handles this new procedural device in practice. Plaintiffs now know approximately how much it costs (in the case at hand, CHF 12,000)[51] and approximately how long it takes (in the case at hand, four months and three weeks).

## 3. Evidentiary Status of Expert Opinions

**18** A critical factor in patent litigation is the evidentiary status of expert opinions. As discussed above (see *supra* para. 2), the Swiss Federal Patent Court does not ordinarily appoint experts, but instead relies on its technical judges to assess technical issues. However, the parties are typically inclined to submit opinions authored by experts of their own choosing or opinions of experts appointed by foreign courts in parallel proceedings taking place abroad. The latter situation has already been brought before the Swiss Federal Patent Court in the context of an invalidity action regarding the Swiss part of a European patent.[52]

**19** In support of the validity of its patent, the defendant submitted two extensive opinions rendered by experts appointed by the German Supreme Court and the Tribunal of Rome, respectively. The plaintiff argued that these opinions were neither expert opinions nor any other type of evidence within the meaning of the Swiss Code of Civil Procedure, whereas the defendant claimed that these opinions qualified as documents and were therefore admissible into evidence.[53] Even though the opinions in question had been commissioned by foreign courts and not by any of the parties, the Swiss Federal Patent Court seized the opportunity to lay down the law on the evidentiary status of opinions authored by party-appointed experts. Not surprisingly, it followed the Supreme Court[54] by concluding that such opinions did not qualify as evidence under Swiss law, but instead as mere party allegations that, while admissible as such, had to be treated as allegations of fact and therefore had to be incorporated into the party briefs in order to be considered by the court.[55]

**20** Turning to opinions commissioned by foreign courts, the Swiss Federal Patent Court held that they were neither party expert opinions nor court expert opinions according to the Swiss Code of Civil Procedure, but rather simple documents to be treated as party allegations, just like party opinions.[56] As a result, these opinions did not have to be considered by the Swiss Federal Patent Court if their contents were not incorporated in detail into the party briefs (as opposed to being incorporated by reference).[57] In the case at hand, since the defendant had merely incorporated the conclusions of the foreign expert opinions into its briefs, the court admitted these opinions only as evidence to prove that the defendant's allegations regarding the content of

these conclusions were accurate, but otherwise disregarded them.[58] While the evidentiary status of opinions that are not authored by experts appointed by the competent Swiss courts may be a comparative anomaly, at least the position of the Swiss Federal Patent Court is now clear.

## II. Substantive Issues

**21** In terms of substantive issues, the Swiss Federal Patent Court had the opportunity to set forth the patent infringement test it intends to use and to apply standard patent doctrine in the context of novelty and non-obviousness decisions.[59] In addition, the Swiss Supreme Court also decided a case relating to the issue of non-obviousness.

### 1. Infringement Test

**22** In one of the first cases regarding a request for a preliminary injunction on the basis of alleged patent infringement, the Swiss Federal Patent Court laid out the test it would use for such requests. Under the general procedural rules, in summary proceedings for a preliminary injunction, the plaintiff has to show the likely existence of (i) an actual or impending act of patent infringement and (ii) irreparable harm arising out of that infringing act.[60] According to the Swiss Federal Patent Court, these rules imply a three-pronged test, namely (i) whether the request for relief contains the concrete technical elements of the accused device to be enjoined, (ii) whether the defendant uses exactly this type of accused device, and (iii) whether said device comes within the scope of protection of the patent in suit, either literally or by virtue of equivalents. If the first prong is not fulfilled, the case is dismissed without prejudice on procedural grounds, as discussed in detail above (see *supra* paras. 9-12). If the second or the third prong is not fulfilled, the request for relief is denied with prejudice. In the context of summary proceedings for preliminary injunctive relief, it is sufficient if the first prong is fulfilled and if the likely existence of the second and third prongs is shown.[61]

**23** In applying this infringement test to the request for preliminary injunctive relief, the Swiss Federal Patent Court also explained that the complete accused device, as defined in the request, must fall within the scope of protection of the patent in suit, because otherwise the request would cover subject matter that is not protected by the patent claims and can therefore not be enjoined.[62] Given that the description of the accused device in the plaintiff's request failed to include a technical element contained in the allegedly infringed patent claim, granting the request would have extended the protection of the patent into the prior art. In other words, the request as filed was overly broad and was therefore denied.[63]

### 2. Novelty

**24** In adjudicating a request for preliminary injunctive relief for patent infringement,[64] the Swiss Federal Patent Court, faced with an invalidity defense, was called to express its views on a particular issue of novelty. More specifically, the patented invention was described in terms of product claims consisting of structural elements combined with indications of the intended purpose of some of these elements.[65] The issue was whether the patented invention was anticipated by a prior art device that consisted of all claimed structural elements, but that had never been suggested to be used for the claimed purposes. Following the practice of the European Patent Office,[66] the Swiss Federal Patent Court reasoned that if the prior art device was in fact *suitable* for the purposes indicated in the relevant patent claim, it would defeat the novelty of the patented invention.[67] In the case at hand, a drilling device for embroidery machines disclosed in a German patent in 1932[68] was found to be suitable for the purposes indicated in the claims of the relevant Swiss patent on a cutting device for embroidery machines.[69] As a result, the relevant claims of the Swiss patent in suit were considered anticipated and therefore invalid.[70] In addition, the infringement of other claims or patents that were potentially valid had not been shown, because the plaintiff had not properly alleged that the defendant had actually used the devices defined in these claims or patents.[71] Accordingly, the request for a preliminary injunction was denied. What is perhaps most notable about this case, for future reference, is that it demonstrates that the Swiss Federal Patent Court is clearly looking to the European Patent Office for guidance on issues of substantive patent law.

### 3. Non-obviousness

**25** In December 2011, the Swiss Supreme Court decided one of its few non-obviousness cases.[72] The plaintiff had filed an action with the Commercial Court of the Canton of St. Gallen to have one of the defendant's Swiss patents on an inductive heating element in a cooking device declared invalid for lack of inventive step. The commercial court denied relief, and the plaintiff appealed to the Swiss Supreme Court, arguing, *inter alia*, that the commercial court had wrongly instructed the court-appointed expert on the basis of the court's erroneous selection of the closest piece of prior art for non-obviousness purposes. The Swiss Supreme Court first reviewed the standard doctrine of non-obviousness in patent law,[73] and then turned to the European

Patent Office's *problem-solution approach* that lay at the heart of the plaintiff's argument. The Court explained that the problem-solution approach is not the only possible method for determining inventive step or non-obviousness, and that, in fact, it should not matter which piece of prior art is chosen as a starting point for the inquiry into whether a person having ordinary skill in the art could have achieved the solution provided by the patent with little intellectual effort or whether doing so required inventive activity.[74] After all, courts cannot solely rely on the closest piece of prior art, but instead have to consider other relevant prior art as well. Therefore, the Swiss Supreme Court ruled that the plaintiff's critique regarding the wrong selection of the closest piece of prior art was unfounded. Moreover, it also explained that while the mere combination of prior art elements or processes was obvious if, when combined, they continued to work in the usual fashion without interaction, the combination was non-obvious if the prior art elements or processes, when combined, produce a new technical result.[75] Applying this distinction to the case at hand, the Swiss Supreme Court affirmed the lower court's decision by holding that the patented invention in question was non-obvious, in part because the prior art did not suggest the technical solution found by the patentee and because some prior art references actually taught away from that solution, making it a surprising find.[76]

**26** The Swiss Federal Patent Court also had the opportunity to apply the law of non-obviousness in 2012, albeit in the context of a request for a preliminary injunction.[77] The plaintiff claimed patent protection on esomeprazole magnesium trihydrate and sued the manufacturer of a drug consisting of esomeprazole magnesium dihydrate, arguing that the defendant's product actually also contained the patented substance. The defendant took the position that the patent was invalid for lack of inventive step, because it was known at the priority date that crystalline esomeprazole magnesium existed in the form of hydrates, so finding a trihydrate form was obvious.[78] Against this background, the Swiss Federal Patent Court explained that the problem-solution approach required the court (i) to identify the closest piece of prior art, (ii) to define the objective technical problem to be solved by the invention, and (iii) to examine whether a person having ordinary skill in the art could not only find, but would also have found the claimed invention.[79] The court referred this question to a technical judge. In her report, she concluded that the claimed invention was obvious, because solving the technical problem of finding new and advantageous forms of esomeprazole magnesium by providing a trihydrate form was part of the professional knowledge of a skilled person working in the field of drug development, particularly in view of a scientific overview article on the subject that was part of the prior art. The technical judge further explained that a person of ordinary skill would have searched for different crystalline forms of a drug, including hydrates, as part of the normal research and development process and would have also routinely used the standard analytic processes to detect hydrate forms.[80] The same is true for the arbitrary selection of a specific form (trihydrate) from a generic group of equally suited candidates (hydrates).[81] The other judges on the panel followed the report by the technical judge, rejecting any and all arguments set forth by the plaintiff. As a result, the request for a preliminary injunction was denied.

**27** It is somewhat remarkable that the Swiss Federal Patent Court did not mention the Supreme Court's non-obviousness case discussed above (see *supra* para. 25). While it is clear that the Supreme Court case did not involve the same technology or address the same issues, it still provided some background on the law of non-obviousness, including the significance of the problem-solution approach. This is a bit unusual, given the fact that the Swiss Federal Patent Court typically shows that it is well aware of what the Supreme Court does. Instead, the only references in the context of non-obviousness are to the Guidelines for Examination in the European Patent Office and to a pertinent decision by an EPO Board of Appeal. In other words, just as in the novelty case discussed above (see *supra* para. 24), the Swiss Federal Patent Court again looked exclusively to the European Patent Office for guidance on matters of substantive patent law. This is not necessarily wrong, and may well make sense in a particular case, especially if European patents are involved, but it does suggest to some extent that the influence of technical judges, who are particularly familiar with the practices of the EPO, may carry a certain risk of undue deference to the European Patent Office. Only time will tell whether the structural make-up of the Swiss Federal Patent Court will have a lasting impact on the direction of its case law.

## C. Conclusion

**28** The year 2012 was an exceptional year for patent law in Switzerland, because it stands for the beginning of a new era in Swiss patent litigation. The Swiss Federal Patent Court has started operating and is on track. The court obviously strives to provide quick and cost-effective proceedings as well as high-quality decisions, and it has done so with remarkable success.[82] It understands the importance of open communication in building confidence in the new system. Aside from issuing its procedural guidelines and publishing its decisions in a timely manner, it has also taken care to provide a bit more detail in its opinions than is customary whenever it deemed it necessary to settle a matter of principle in order to increase legal certainty for the future. Specifically,

the court has provided guidance on the evidentiary status of party expert opinions, the formal requirements for requests for injunctive relief, the infringement and non-obviousness tests it employs, the use of reports and statements from technical judges in lieu of expert opinions, and the procedural devices for the pre-trial taking of evidence, in particular the new patent-specific device of precise description. Moreover, the president of the court speaks regularly at conferences in order to educate attorneys, patent attorneys, and in-house counsel on practicing before the court. If the enthusiasm about the court and the commitment of the judges to make it work persist, the Swiss Federal Patent Court will have the potential of becoming a competitive alternative to the planned unified patent system of the European Union.[83] Looking forward, it will be interesting to see whether the relatively strict formal requirements for requests for injunctive relief will lead to increased numbers of requests for precise description of allegedly infringing devices or processes. Finally, on a more structural note, it remains to be seen whether the institutional choice of using technical judges, combined with the paramount importance of their often outcome-determinative reports and statements, will substantively transform Swiss patent jurisprudence towards a more automatic adoption of the practices and case law of the European Patent Office.

■

1 For an overview of the new Swiss patent litigation system in English, see *Rigamonti*, The New Swiss Patent Litigation System, JIPITEC 2011, 3; see also *Ritscher*, Patent Litigation in Switzerland – At the Brink of a New Era, in Hansen & Schüssler-Langeheine (eds.), Patent Practice in Japan and Europe, Alphen aan den Rijn 2011, 211-219. For overviews in German and French, see *Stieger*, die Zuständigkeit der Schweizer Gerichte für Prozesse über und im Zusammenhang mit Patenten ab 2011, sic! 2010, 3; *Stieger*, Prozessieren über Immaterialgüterrechte in der Schweiz – ein Quantensprung steht bevor, GRUR Int. 2010, 574; *Bosshard*, Le nouveau Tribunal fédéral des brevets et les jurisdictions cantonales, SZZP 2010, 191; *Gick-Komondy*, Schweizerische Patentgerichtsbarkeit im Vergleich mit der europäischen Entwicklung, Diss. Bern, Zurich 2010, 189-213; *Schweizer*, Das neue Bundespatentgericht: besser, schneller, billiger?, Jusletter 12. März 2012; *Bremi*, Das Schweizer Bundespatentgericht – ein neuer schneller Weg zu Verletzungsurteilen in Europa, Mitt. 2012, 529.

2 See *Rigamonti*, The New Swiss Patent Litigation System, JIPITEC 2011, 3, paras. 9 and 58.

3 The Swiss Federal Patent Court currently consists of two full members of the Court, a legally trained full-time judge (the President of the Court) and a technically trained part-time judge, as well as 11 legally trained and 25 technically trained adjunct judges who work as attorneys and patent attorneys (in US terminology, patent agents) and are called to serve on the court on a case-by-case basis.

4 Note that the Swiss Supreme Court has held that, if a factual issue is in dispute between the parties and if the court itself does not possess the required technical expertise to decide the issue, it is arbitrary *not* to appoint a technical expert and to merely rely on party-appointed experts; see BGE 132 III 83, consid. 3.5; see also BGE 129 III 25, consid. 3; BGer. 4A_52/2008 of 29 April 2008, consid. 3.4. Under the old system, the use of such court-appointed technical experts was, therefore, necessary as a matter of law. Under the new system, however, technical judges alleviate the need for court-appointed experts.

5 According to estimates presented by the President of the Swiss Federal Patent Court at a conference for practitioners held in St. Gallen on 5 December 2012, the creation of a report by a technical judge is about 12 times faster and costs about one half to two thirds less than the creation of a report by a court-appointed expert.

6 See *Bremi*, Das Schweizer Bundespatentgericht – ein neuer schneller Weg zu Verletzungsurteilen in Europa, Mitt. 2012, 529, 532.

7 For more details, see also *Rigamonti*, Ein Jahr schweizerisches Bundespatentgericht, ZVglRWiss 2013 (forthcoming).

8 See also *Bremi*, Das Schweizer Bundespatentgericht – ein neuer schneller Weg zu Verletzungsurteilen in Europa, Mitt. 2012, 529, 531.

9 See *Rigamonti*, The New Swiss Patent Litigation System, JIPITEC 2011, 3, para. 59.

10 Note that decisions by the Swiss Federal Patent Court can be appealed to the Swiss Supreme Court as a matter of right without exception; see *Rigamonti*, The New Swiss Patent Litigation System, JIPITEC 2011, 3, para. 9.

11 Note that Switzerland does not have a bifurcated system for infringement and validity. Both issues are decided by the Swiss Federal Patent Court in a single proceeding.

12 For a more comprehensive review, see *Rigamonti*, Ein Jahr schweizerisches Bundespatentgericht, ZVglRWiss 2013 (forthcoming).

13 See also *Bremi*, Das Schweizer Bundespatentgericht – ein neuer schneller Weg zu Verletzungsurteilen in Europa, Mitt. 2012, 529, 531-532.

14 See Art. 8 of the Guidelines on Proceedings before the Federal Patent Court.

15 Note that neither the court nor the parties are allowed to later refer to or use anything that was said during the informal part of the hearing.

16 See BGer. 4A_175/2012 of 3 April 2012; for proceedings below, see BPatGer. O2012_012 of 20 February 2012. This case involved a pro se plaintiff who was apparently unwilling to comply with standard procedural rules governing the filing of a court action.

17 See BGer. 4A_443/2012 of 5 February 2013; for proceedings below, see BPatGer. O2012_021 of 7 June 2012. The case involved the question of whether the Swiss Federal Patent Court has subject matter jurisdiction over a claim brought by a foreign company against the Swiss government for the alleged infringement of a patent in the federal administration of a toll system for trucks. The Swiss Federal Patent Court held that it had jurisdiction to hear both the request for injunctive relief and the request for damages. The Swiss Supreme Court held that while the Swiss Federal Patent Court had jurisdiction to hear the request for injunctive relief, it lacked jurisdiction to adjudicate the claim for damages.

18 For details, see *Rigamonti*, Ein Jahr schweizerisches Bundespatentgericht, ZVglRWiss 2013 (forthcoming).

19 BGE 131 III 70, consid. 3.3.

20 BGE 131 III 70, consid. 3.4.

21 See BPatGer. S2012_002 of 7 March 2012, consid. 2; see also BPatGer. O2012_004 of 24 August 2012, consid. 9; BPatGer. S2012_003 of 2 February 2012, consid. 15.

22 See BPatGer. S2012_002 of 7 March 2012, consid. 3; see also BPatGer. O2012_004 of 24 August 2012, consid. 9.

23 BPatGer. O2012_004 of 24 August 2012, consid. 9.

24 See, e.g., *Widmer/Degen*, Anmerkung zu BGE 131 III 70, sic! 2005, 211, 212; *Walter*, Die bundesgerichtliche Rechtsprechung im Jahr 2005, ZBJV 2006, 580, 602.

25 See also *Widmer/Degen*, Anmerkung zu BGE 131 III 70, sic! 2005, 211, 213-214.

26 See Art. 77(1)(b) of the Swiss Patent Act; on this procedural remedy, see *Rigamonti*, The New Swiss Patent Litigation System, JIPITEC 2011, 3, paras. 56-57.

27 BPatGer. S2012_005 of 13 June 2012, consid. 11.1.

28 BPatGer. S2012_005 of 13 June 2012, consid. 11.1.

29 BPatGer. S2012_005 of 13 June 2012, consid. 11.2.

30 BPatGer. S2012_005 of 13 June 2012, consid. 12.1 and 12.3.

31 See *Rigamonti*, The New Swiss Patent Litigation System, JIPITEC 2011, 3, paras. 53-57; see also *Schweizer*, Vorsorgliche Beweisabnahme nach schweizerischer Zivilprozessordnung und Patentgesetz, ZZZ 2010, 3.

32 See Art. 158(1)(b) of the Swiss Code of Civil Procedure.

33 See Arts. 77(1)(b) and 77(4) of the Swiss Patent Act.

34 BGE 138 III 76; for brief comments on this case, see *Schweizer*, Anmerkung zu BGE 138 III 76, sic! 2012, 334; *Berger*, Entwicklungen im Immaterialgüter- und Lauterkeitsrecht, SJZ 2012, 401, 402.

35 In this context, it should be noted that it is a key feature of the Swiss law of appellate procedure that first-instance decisions on preliminary measures are not subject to *de novo* review, but instead are reviewed for the violation of constitutional rights only (Art. 98 of the Act on the Federal Supreme Court), such as the right to be heard or the prohibition of arbitrariness, which is a very high standard of review; see also generally *Rigamonti*, Ein Jahr schweizerisches Bundespatentgericht, ZVglRWiss 2013 (forthcoming).

36 BGE 138 III 76, consid. 2.4.1.

37 BGE 138 III 76, consid. 2.4.2.

38 BGE 138 III 76, consid. 2.4.2.

39 BPatGer. S2012_006 of 27 April 2012, consid. 1.

40 On the test used by the Swiss Federal Patent Court, see BPatGer. S2012_006 of 27 April 2012, consid. 5.

41 BPatGer. S2012_006 of 27 April 2012, consid. 6.

42 BPatGer. S2012_006 of 27 April 2012, consid. 7.

43 BPatGer. S2012_006 of 27 April 2012, consid. 7.

44 Arts. 77(1)(b) and 77(2)-(5) of the Swiss Patent Act. See also, in general, *Rigamonti*, The New Swiss Patent Litigation System, JIPITEC 2011, 3, paras. 56-57; *Ritscher*, Patent Litigation in Switzerland – At the Brink of a New Era, in Hansen & Schüssler-Langeheine (eds.), Patent Practice in Japan and Europe, Alphen aan den Rijn 2011, 216-217; *Calame*, Beweissicherung im Zusammenhang mit Patentverletzungsklagen in der Schweiz ab 2011, in Liber Amicorum Rudolf Tschäni, Zurich 2010, 494-504; *Schweizer*, Der Anspruch auf genaue Beschreibung gemäss Art. 77 PatG, sic! 2010, 930.

45 But see Art. 158(1)(b) [first variant] of the Swiss Patent Act; for the old law, see also *Calame*, Beweissicherung im Zusammenhang mit Patentverletzungsklagen in der Schweiz ab 2011, in Liber Amicorum Rudolf Tschäni, Zurich 2010, 491-492.

46 Art. 77(2) of the Swiss Patent Act.

47 BPatGer. S2012_007 of 14 June 2012, consid. 3.

48 BPatGer. S2012_007 of 14 June 2012, consid. 4.

49 To the extent that the plaintiff's attorneys and patent attorneys learned of facts during the precise description that the court did not later share with the plaintiff, the duty of confidentiality continues to exist; BPatGer. S2012_007 of 14 June 2012, consid. 5.

50 See, e.g., BGH, GRUR 2010, 318; see also *Meier-Beck*, Die Rechtsprechung des Bundesgerichtshofs zum Patent- und Gebrauchsmusterrecht im Jahr 2009, GRUR 2010, 1041, 1046 f.; *Müller-Stoy*, Der Besichtigungsanspruch gemäss § 140c in der Praxis – Teil 2, Mitt. 2010, 267, 270; *Ritscher*, Patent Litigation in Switzerland – At the Brink of a New Era, in Hansen & Schüssler-Langeheine (eds.), Patent Practice in Japan and Europe, Alphen aan den Rijn 2011, 217; *Schweizer*, Der Anspruch auf genaue Beschreibung gemäss Art. 77 PatG, sic! 2010, 930, 933-934.

51 BPatGer. S2012_007 of 23 August 2012, consid. 7. Note, however, that this figure does not include the fees of attorneys and patent attorneys.

52 BPatGer. O2012_022 of 3 May 2012.

53 BPatGer. O2012_022 of 3 May 2012, consid. 7.

54 See BGE 132 III 83, consid. 3.4.

55 BPatGer. O2012_022 of 3 May 2012, consid. 10.1.

56 BPatGer. O2012_022 of 3 May 2012, consid. 10.2 and 10.3.

57 BPatGer. O2012_022 of 3 May 2012, consid. 10.4.

58 BPatGer. O2012_022 of 3 May 2012, consid. 10.5. Regarding the implementation of this point, see also BPatGer. O2012_022 of 31 July 2012.

59 The Swiss Federal Patent Court also decided a patent ownership dispute, but it is too fact-specific to merit an in-depth discussion. Basically, the issue was whether the University of Bern had rights to an invention that one of its employees had made jointly with an outside engineer. The Swiss Federal Patent Court held that the University of Bern could not show any transfer of rights from the Canton of Bern, its predecessor entity, and that there had been no legal basis for the transfer of the rights from its employee, in addition to the University having forfeited the action for the assignment of patent rights; see BPatGer. O2012_010 of 28 March 2012.

60 See Art. 77 of the Swiss Patent Act in conjunction with Art. 261(1) of the Swiss Code of Civil Procedure.

61 BPatGer. S2012_003 of 2 February 2012, consid. 14. The infringement test adopted by the Swiss Federal Patent Court corresponds verbatim to the infringement test used by the Commercial Court of the Canton of Zurich; see, e.g., HGer. ZH, HE110003-O of 21 January 2011, consid. 3.

62 BPatGer. S2012_003 of 2 February 2012, consid. 14.

63 BPatGer. S2012_003 of 2 February 2012, consid. 15.

64 BPatGer. S2012_004 of 24 March 2012.

65 See Patent No. CH 701 638 B1, Claim 1.

66 See *European Patent Office*, Case Law of the Boards of Appeal of the European Patent Office, 6th ed., Munich 2010, 184-185; see also Guidelines for Examination in the European Patent Office, 2012, ch. F-IV-18, para. 4.13.

67 BPatGer. S2012_004 of 24 March 2012, consid. 8.

68 See Patent No. DE 566 263.

69 BPatGer. S2012_004 of 24 March 2012, consid. 9.

70 BPatGer. S2012_004 of 24 March 2012, consid. 10. The same was true for another patent claim invoked by the plaintiff (consid. 13).

71 BPatGer. S2012_004 of 24 March 2012, consid. 15-16.

72 BGE 138 III 111.

73 BGE 138 III 111, consid. 2.1.

74 BGE 138 III 111, consid. 2.2.

75 BGE 138 III 111, consid. 2.3.

76 BGE 138 III 111, consid. 2.3 and 2.4.

77 BPatGer. S2012_011 of 21 November 2012.

78 BPatGer. S2012_011 of 21 November 2012, consid. 4.

79 BPatGer. S2012_011 of 21 November 2012, consid. 4.4.

**80** BPatGer. S2012_011 of 21 November 2012, consid. 4.5.

**81** BPatGer. S2012_011 of 21 November 2012, consid. 4.5 and 4.6. See also EPO Board of Appeal, Case No. T 777/08 of 24 May 2011, consid. 5.2.

**82** See also *Bremi*, Das Schweizer Bundespatentgericht – ein neuer schneller Weg zu Verletzungsurteilen in Europa, Mitt. 2012, 529, 530; *Berger*, Entwicklungen im Immaterialgüter- und Lauterkeitsrecht, SJZ 2012, 401, 402.

**83** See Agreement on a Unified Patent Court, EU Council Doc. No. 16351/12 of January 11, 2013; see also Regulation (EU) No 1257/2012 of the European Parliament and of the Council of 17 December 2012 implementing enhanced cooperation in the area of the creation of unitary patent protection, OJ EU L 361 of December 31, 2012, p. 1; Council Regulation (EU) No 1260/2012 of 17 December 2012 implementing enhanced cooperation in the area of the creation of unitary patent protection with regard to the applicable translation arrangements, OJ EU L 361 of December 31, 2012, p. 89.

# Christophe Geiger (ed.), Criminal Enforcement of Intellectual Property. A Handbook of Contemporary Research

Edward Elgar 2012, 416 pages, ISBN 978-1-84980-146-1

by **Rita Matulionyte,**
Dr. iur., LL.M., Deputy Director at Law Institute of Lithuania



Recommended citation: Rita Matulionyte, Book Review – Christophe Geiger (ed.), Criminal Enforcement of Intellectual Property. A Handbook of Contemporary Research, 4 (2013) JIPITEC 63, para. 1.

**1** Criminal enforcement of IP rights has been a hot topic on both the European and international level for the last several years. Despite the failure of the Proposed EU Directive on Criminal Measures (2005/0127/COD) and the rejection by the European Parliament of the Anti-Counterfeiting Trade Agreement (ACTA) that contained provisions on criminal enforcement (among others), the discussion has not stopped. Europeans are awaiting with concern new promised initiatives in this field from the European Commission, and the international IP society is following the negotiations of the Trans-Pacific Partnership agreement. Therefore, the research handbook 'Criminal Enforcement of Intellectual Property', edited by *Christophe Geiger*, is a timely academic venue to cultivate the ground for the on-going and upcoming battles in this field.

**2** The book contains contributions by the most prominent researchers in the field of IP from Europe (Germany, France, UK, Finland) and abroad (US, China, Argentina). The book is arranged in three parts addressing societal issues underlying IP enforcement (I), the search for right remedies for IP enforcement (II) and a selection of the most problematic issues (III). Part II is the richest, ranging from historical and economic perspectives to criminal IP enforcement to international, regional and national experiences in this field. By starting from general arguments and finishing with specific problems, and by including an interdisciplinary approach, the book provides a broad picture of the discussion surrounding criminal enforcement in IP. Readers could be disappointed that some of the most recent developments – such as the rejection of ACTA in the European Parliament, the discussion surrounding the Trans-Pacific Partnership agreement or the fresh experience in the implementation of the controversial French HADOPI law – are not covered by the book (the manuscript was probably submitted to the publisher before these events). Also, keeping in mind the prospective initiative by the European Commission on criminal measures, readers might have expected some more concrete suggestions on how Europe has to move forward on this issue. Overall, however, the contributions are of high academic value and are likely to be instructive and enlightening for both beginners and experts in the field.

**3** Each contribution deserves a short notice. The authors of the first part seem to argue that an over-strict protection of IP does not necessarily meet the needs of society. *Retro M. Hilty,* while discussing economic, legal and social impacts of counterfeiting, suggests that imitations of (patented) products, as distinguished from identical use, are good for competition and innovation and therefore should not be punished. Also, as the boundary between (welcomed) imitations and (unwelcomed) identical use is not clear, a very strong enforcement of the latter (e.g. through criminal measures) can be a deterrent for the former as well as to competition in the markets in general. The same argument in the field of trademarks and copyrights, however, seems to be underdeveloped. *Ansgar Ohly* provides an excellent analysis of whether IP law should also protect the interests of consumers. Ohly suggests a wisely differentiated answer: in the case of patent and copyright, he does not see such a need; however, in regard to trademark law, he concludes that 'consumer interests cannot be ignored', and the inclusion of consumer protection as one of the goals

in the EU trademark law would be advantageous for right holders as well as users. In this way, the author does not entirely reject the 'consumer interest' argument currently often heard in IP enforcement discussions, but puts justified limits on it.

**4** The next contribution by *Duncan Matthews* sets similar limits to the 'public health' argument ('counterfeit medicines are dangerous to public health'), which is also currently often (mis)used in IP enforcement debates. He demonstrates that it is not so much the counterfeit medicines that threaten public health but rather falsified medicines. The latter should be dealt with by drug regulatory and supervisory authorities and not by IP enforcement agencies. In addition, the author demonstrates that the definition of 'counterfeiting' is currently too broad (both in public discussion and law); this is also seen from the famous Dutch case on generic drugs in transit. The latter case is an example of how the over-broad concept of counterfeit products, as defined by EU law, and over-strict enforcement may have negative effects on public health – instead of positive ones that IP enforcement is expected to have. *Carlos M. Correa* seeks to demonstrate that strong enforcement of IP counterfeiting in developing countries is unreasonable. The contribution sums up the main arguments put forward by opponents of strong enforcement (such as the unreliability of counterfeiting figures indicated by industries, the misuse of 'consumer protection' and 'public health' arguments, the advantages of counterfeiting for both consumers and right holders, etc.). Readers familiar with the discussion may miss some new arguments or some constructive proposals as to how the balance between different interests could be drawn. The last contribution in the section by *Mickaël R. Roudaut* is a good contrast to all the previous ones. Advocating a strong pro-enforcement stance, the representative from the European Commission uses sharp language and comparisons (e.g. 'an evolving phenomenon invested in by organized crime (as well as terrorism funding channels*), counterfeiting kills'* (p. 75); 'digital piracy has, in less than a decade, transformed the movie and music industries *while the European navies are boarding ships loaded with cocaine'* (p. 76) – *italics* by RM). He further provides some 'crude and simplistic' (as the author himself recognizes) estimates of counterfeiting and some strong conclusions (counterfeiting as 'the main illegal market after narcotics' (p. 79)). Although much of what is said lacks authoritative support, the article also cites some interesting reports, statistics and statements by EU officials on the relationship between counterfeiting and organized crime.

**5** Part II starts with historical, economic and moral perspectives on criminal enforcement. *David Lefranc* demonstrates that in France, both before and immediately after the French Revolution, the laws provided for criminal enforcement of IP rights, with the strongest punishments for trademark infringement. Readers might also have been interested to read about more recent developments (e.g. in the 20th century) in order to understand the rationale behind current criminal provisions. The contribution by *Andrea Wechsler* demonstrates the difficulties in evaluating the criminal enforcement of IP rights from an economic approach. Although the conclusions may appear disappointing ('learnings from economics of crime and punishment are not necessarily transferable to the realm of IP law' (p. 149)), such a careful approach is wise and opens space for further discussion. *Alexander Peukert* contributes to the interdisciplinary discussion with an interesting question: Why do 'good people' disregard copyright on the Internet? Apart from legal reasons (insufficient legal certainty), he points to the psychological argument of 'moral disengagement': users reconstruct their conduct as having a moral purpose in order to make it socially acceptable (e.g. to share information or to teach record companies that their prices are too high). The author concludes that 'good people' are already frustrated with the conflict between what is right (using their own right to freedom of speech and expression) and what is wrong (infringement of copyright); therefore, criminal measures against their conduct would only lead to even more frustration and ignorance of copyright.

**6** Another set of articles provides an analysis of international, European and national legal frameworks in the field. With a focus on the WTO China-IPRs case, *Henning Grosse Ruse-Khan* analyses the scope and limits of Article 61 of TRIPS and then looks at how far ACTA modifies the international framework set by TRIPS. The contribution demonstrates that ACTA has gone considerably – and unreasonably – beyond the flexible international minimum standards as set by TRIPS. Next, *Jonathan Griffiths* looks at criminal enforcement of IP in the EU from the perspective of human rights. He first asks whether IP rights, given their fundamental right status under EU law, should be enforceable by criminal laws; with arguments that are perhaps a bit too general, he gives an answer: no. Then he provides a preliminary survey of human rights issues that may be important when extending criminal enforcement to IP (e.g. disproportionate sentences, monitoring of Internet communication and the rights to privacy and freedom of expression). These tips might be useful for EU lawmakers if they (dare to) propose a new draft for the EU Directive on Criminal Measures, though a deeper analysis of each issue (or selected ones) would have given more value to the work.

**7** *Tuomas Mylly* addresses the issue of (changing) EU competences in harmonizing criminal law – one of the most important issues during the debates on both the EU Criminal Measures Directive and ACTA. The contribution analyses in detail the new competences

of the EU in criminal law (after the Lisbon Treaty), its limits, and the means to challenge them (e.g. the emergency brake procedure and the protocol on subsidiarity principle). The author in particular highlights an extremely rapid growth of the EU external competences in criminal enforcement of IP (i.e. signing bilateral or international agreements) and the fact that their scope is even broader than in cases of internal competence (some measures such as the emergency brake procedure are not available here). Finally, *Johanna Gibson* gives an overview of the legislative history of the Proposed Directive on Criminal Measures and sums up some of the critical points of the Proposal (she also gives a short overview of the criminal provisions of ACTA). A bit disappointingly, the sub-section on European developments in criminal law finishes without providing any more concrete suggestions or guidelines for the new Commission's initiatives in this regard.

**8** Three more contributions discuss national experiences in criminal enforcement of IP. *Daniel Gervais* compares Canada and the US in this regard. Whereas in Canada the generally available criminal measures are rarely applied in practice, in the US (not surprisingly) their scope and practical importance has been expanding. It is interesting to read how the 'commercial use' requirement in the US has been gradually expanded in copyright cases and now even includes file-sharing activities. Meanwhile, *Peter K. Yu* focuses on the implementation of TRIPS criminal enforcement standards in developing countries, in particular, China. His contribution illuminates the background of the WTO China-IPRs dispute as well as arguments of the parties and the WTO panel, and provides a deep analysis of the decision and its rationale, with useful explanations about the Chinese legal system, its history, recent developments and remaining shortcomings.

**9** *Guido Westkamp* presents the situation in the UK. The author convincingly argues that due to the ever-expanding scope of trademark under the jurisprudence of the Court of Justice of the European Union (CJEU), criminal liability for trademark infringements has also dangerously expanded (at least if the relevant criminal provision is read literally). As far as copyright is concerned, he argues that under the recent UK Digital Economy Act 2010 (which allows disconnecting infringing users from the Internet), 'users are effectively criminalized given that rather severe sanctions may be imposed on the basis of a lofty description of "copyright infringement"'. He further insightfully discusses numerous criticisms of the 2010 Act and provides more general arguments against criminalization of IP law. The overview of national experiences finishes with the contribution about France written by *Joanna Schmidt-Szalewski*. Disappointingly, in seven pages of descriptive (and, in numerous instances, imprecise and unclear) text, the author merely points to the main historical statutes imposing criminal liability in France, and reiterates the contents of the EU Proposed Directive on Criminal Measures. Keeping in mind that France is known as the country with one of the most protectionist policies towards IP, readers would have been especially interested to hear more about criminal enforcement policies and practice in this country. Certain compensation for this is offered in the last contribution by Christophe Geiger, at least in relation to copyright enforcement online (see below).

**10** The last part of the book deals with selected enforcement issues, namely in the fields of drugs, spare parts and copyright online piracy. The report on comparative research on criminal enforcement of counterfeit drugs, as presented by *Hans-Georg Koch*, touches upon various issues of criminal enforcement of counterfeit drugs, from the definition, design and content of criminal provisions in national laws, to international prosecution and organized crime issues. Although readers may have expected more extensive remarks and conclusions on each of the issue (or at least a link to a full study), each section contains some useful and interesting proposals on how to improve national criminal laws in the field. One of the most interesting suggestions is 'a certain criminalization' of the online purchaser of counterfeit drugs – more elaboration on this would have been helpful. *Josef Drexl* contributes an excellent piece which convincingly demonstrates that there is no justification for maintaining design protection for spare parts, since it provides a standard example of anti-competitive IP law. Accordingly, he suggests that the Proposed Directive on Criminal Measures should clearly exclude from criminal liability violations of design protection for spare parts. As the last contribution, *Christophe Geiger* comments on a famous French HADOPI law. After an interesting and instructive pre-history of the HADOPI law, the author sums up numerous criticisms against the HADOPI system that were already articulated in academic and civil groups circles (such as difficulties in establishing infringement, huge costs, uselessness for authors, outdated technology and ineffectiveness in reducing piracy). Since it has been almost three years since the law came into force and there are (at least unofficial) reports on its results, readers would also have been interested to read more about whether the predicted shortcomings are already felt in practice.

**11** Overall, the book should be welcomed and complimented for giving a broad and simultaneously rather detailed picture of the discussion on criminal enforcement of IP. Written by highly prominent researchers from around the world and covering a wide range of issues, it could serve as a good basis for opposing active industry lobbying for ever stronger IP enforcement and for arguing in favour of a more balanced approach to IP.

# Editors' Pick

In this new column, which from now on shall appear at regular intervals, the editors of JIPITEC would like to present to their readers monographs that in their mind are either outstanding or are worth being mentioned and recommended to the interested reader. Each individual editor is responsible for his or her own choice and each text reflects personal interests and preferences rather than an editorial policy.



Recommended citation: T. Dreier, L. Guibault, A. Metzger, M. Peguera, Editors' Pick, 4 (2013) JIPITEC 66, para. 1

**1** To open this new format, *Thomas Dreier*[*] would like to draw attention to a monograph by

> **Zech, Herbert: *Information als Schutzgegenstand*. Series "JusPriv" No. 166. Mohr Siebeck. Tübingen 2012. XXV, 488 pp.**

**2** After having written his habilitation at the University of Bayreuth within the framework of the university's graduate school, "Geistiges Eigentum und Gemeinfreiheit," Prof. Zech has joined the law faculty of the University of Basel in Switzerland, where he now teaches civil law and IP law, with a focus on intellectual property in life sciences. Writing a second academic monograph after a dissertation in order to qualify for the career path of tenured professorship at a law faculty is still a particular feature of German academic tradition. Working on a habilitation may be a long and, at times, tedious exercise, but it has resulted in quite a number of books that go well beyond a more or less superficial analysis of isolated legal issues.

**3** Of course, Zech is not the first author in Germany to devote his attention to the analysis of the legal protection of information. Rather, with regards to German legal literature in the area of civil law, Zech can tie in with earlier works by Wiebe, Dreier, Haedicke, Peukert and others. In Switzerland and Austria the works by Druey and, more recently, by Mayer-Schönberger can be mentioned. Following in the tradition of Wiebe – from whom Zech has borrowed the title of his work and who already in 1995 undertook the first attempt to characterize information as an "object of protection" – Zech now widens the view and also discusses exclusive protection schemes for information other than through intellectual property rights. Thus, personality rights, the protection of trade secrets, rules against unfair competition (in particular, the protection against unfair product imitation) and property legislation governing rights with regard to the physical embodiment of information likewise come into focus. By this approach, it becomes clear that even in continental European law tradition, rights with regard to information – including intellectual property rights – can much better be described as a bundle of different rights vis-à-vis third persons, rather than one solitary right of property with regard to a particular object. In this respect, the term "allocation" ("Zuordnung") of exclusive rights or even goods likewise becomes less monolithic and more flexible or fluid than it has been traditionally been understood in German legal literature. Of course, on the one hand, the approach chosen to examine the exclusivity of rights with regard to information only indirectly focuses on the communicative aspect of information. However, on the other hand, the notion of information is understood by Zech in a broad sense to cover all information goods such as news, images, gene sequences or stored data.

**4** In an introductory part, the book provides an excellent overview of the state of discussion in German legal literature regarding property and/or exclusive rights concerning information. Then, borrowing from Benkler and Lessig, who distinguish content layer, code layer and physical layer of information, as his central thesis Zech proposes to classify the legal protection schemes for information according to information's characteristics as semantic, syntactic and structural. Whereas semantic information is characterized by its inherent meaning, syntactic information can be described as the signs representing semantic information. Ultimately, structural information is information in its physical embodiment. This differentiation

allows Zech to describe in a new way, for example, the difference between, on the one hand exclusive protection by patent law and on the other hand, by copyright law. From an intellectual property rights perspective, both inventions and works may appear as public goods in need of artificially created exclusivity in order to provide incentives to innovate and create. From Zech's point of view, however, it becomes clear that patent law protects semantic information whereas copyright law only protects syntactic information. Also, the difference between copyright in works and neighboring rights in, for example, phonograms becomes much clearer since the latter protect structural information. This distinction in semantic, syntactic and structural information, including its overlaps in complex information products and services, allows for a rather detailed analysis of existing exclusive protection with regard to its legal commonalities as well as its anomalies.

**5** Also, the reasoning behind granting full or partial exclusivity over access to or re-use of information becomes apparent. Examining, in the second part of his book, in great detail both these reasons for protection as well as the different legal protection schemes currently in existence with regard to semantic, syntactic and structural information, Zech reflects upon rights granted to entities as varied as persons, business secrets, inventions, news, images, genetic sequences, image and sound recordings and stored data. Here, for example, Zech demonstrates that the greatest restriction results from the allocation of exclusivity to semantic information, whereas the amount of restriction decreases from the allocation of exclusivity to syntactic information to the allocation of exclusivity to structural information. Also, he objects to granting neighboring rights protection for semantic information, and he refuses to recognize a right to the immaterial outer appearance of a physical object against being photographed since this would amount to exclusivity for syntactic information based on property law protecting material objects. Besides this, there is much more to discover on information in this book. In sum, Zech's aim is to systematize the existing exclusive rights granted on various legal grounds to information, rather than to create new rights.

**6** Following, *Lucie Guibault* would like to draw the reader's attention to a monograph by:

> **Elkin-Koren, Niva, and Salzberger, Eli M.: *The Law and Economics of Intellectual Property in the Digital Age – The limits of analysis*. Routledge Research in Intellectual Property. London and New York 2013. 286 pp.**

**7** It took almost a decade for the authors to write this book from the moment that the Netherlands Organisation for Scientific Research (NWO) funded the research. But the waiting has paid off: the book takes a refreshing, in-depth, but non-conventional and critical look at the law and economics of intellectual property. For any skeptic of law and economics, it is a joy to read about the "limits of analysis" and to explore with the authors how the traditional analytical framework finds application – or not – in the digital age. The book is built on the premise that while "law and economics discourse has become dominant in intellectual property policy-making, causing policy-makers to focus exclusively on the economic ramifications of intellectual property," this narrow economic perspective leaves out many aspects of creativity and innovation. The authors refer more specifically to the sociology of arts and science or the complexity of human motivation that could be crucial to policy-making in this area. Elkin-Koren and Salzberger's book offer a reconstruction of existing scholarship and methodologies in law and economics so as to address fundamental issues that are traditionally left outside the scope of inquiry. From this perspective, it is probably a good thing that the book was not published ten years ago. Ten years are an eternity in digital terms! The analysis would, therefore, not have been as rich without taking into account such significant socio-economic phenomena as the unstoppable flow of peer-to-peer file sharing, the rise and fall of digital rights management, or the increased popularity of the open content movement, to name but three.

**8** The book is actually quite entertaining as the authors debunk all major tenets of mainstream law and economics analysis, ranging from the assumption of wealth maximization as a basis for positive and normative analysis (leading to an inner incoherence between the two, since the "positive analysis cannot predict the adoption of its normative recommendations"), to the assumption of rationality and exogenous preferences (which "ignores the deficiencies of the shift from assuming self-maximization of utility to assuming self-maximization of wealth"), and to the assumption that the state of technology is fixed (which "overlooks the interdependency and reciprocity between technological developments and legal rules"). Of course, law and economics does have value as a method of legal research for it transcends national boundaries and particularisms in scholarly legal communication. However, mainstream scholarship in law and economics has become, over the years, impregnated by an increasing dose of dogmatism. Elkin-Koren and Salzberger offer this book in an attempt to bring law and economics back on the path of pragmatism.

**9** The road to pragmatism wanders forth further in the book along the core elements of the normative analysis, namely the incentive paradigm and the proprietary model of intellectual property. The discussion on the incentive paradigm is particularly captivating, as the authors illustrate how, in the digital age inhabited by social media, the objects of incentives have shifted from incentives to create, to incentives to disseminate and distribute, to disclose, or to improve — each activity justifying a different form and scope of IP rights, in order to secure the desirable monetary incentives. The path to pragmatism continues its course through the meanders of private ordering, which seems to have become the main form of shaping IP rights. While new forms of private ordering keep emerging, for example through open access initiatives, the question arises whether this type of non-institutional "law-making" is desirable from a social welfare point of view. The same remark holds true regarding the phenomenon of governance by technology, where "law-making" occurs through the tweaking of digital rights management systems. The book concludes with a positive analysis of intellectual property law, examining the role of legislation from different perspectives as well as the role of courts in shaping legal policy toward intellectual property.

**10** All in all, Elkin-Koren and Salzberger's book makes a convincing contribution to the scholarly writings on the law and economics of intellectual property. And the fact that their approach is overwhelmingly, even if inevitably, American should not be an obstacle to its enjoyment.

**11** As regards his turn, *Axel Metzger* would like to suggest

> **Ohly, Ansgar (ed.): *Common Principles of European Intellectual Property Law*. Mohr Siebeck 2012. 272 pp.**

**12** This volume presents a collection of papers given at a conference held in Bayreuth in 2009. The aim of the volume is ambitious, since the concept of "common principles" is based on two analytic perspectives: (1.) Are there any principles common to all or some intellectual property rights, e.g. copyright, patent, trademark, etc. (2.) Are there common European principles of this type? (see the introduction by Ansgar Ohly). The first analytic perspective stands in the tradition of the general parts of codifications, which summarize the general principles applicable to the various specific subject matters covered by the codification, e.g. the famous "Allgemeiner Teil" of the German Civil Code or similar parts of other civil codes, e.g. of Brazil, Greece, Japan, Poland or Russia.[1] The second analytic perspective of common "European" principles follows the model of the working groups and projects in the field of European private law. Because intellectual property has been harmonized intensively by the European Union in the last decades, the contributions to the book follow rather the paradigm of the Acquis Group (on this group see the paper of Gerhard Dannemann) than comparative law projects like the (Lando) Commission on European Private Law.

**13** This twofold abstraction – over different intellectual property rights and different jurisdictions – is reflected by the subjects covered by the authors. Most papers examine subjects of a rather theoretical and method-oriented interest, e.g. "How far does the incentive paradigm carry?" (Alberto Muso); "Two tiered protection – designs and databases as legislative models" (Annette Kur); "The exhaustion of rights and common principles of European intellectual property law" (Jens Schovsbo); "Limitations and exceptions: Towards a European 'fair use' doctrine?" (Jean-Luc Piotraut); and "Fundamental rights as common principles of European (and international) intellectual property law" (Christophe Geiger). But there are also contributions that strive at more concrete questions, especially where horizontal European instruments covering different intellectual property rights have been enacted, e.g. "Common principles of secondary liability?" (Matthias Leistner) and "The European principles of intellectual property enforcement: Harmonisation through communication?" (Markus Norrgård). A special section of the volume contains three papers on the relation of competition law and intellectual property (Steven Andermann, Dirk Visser, Vyautas Mizaras).

**14** After reading the contributions, it becomes obvious that the principles common to the various European intellectual property rights must be understood as (very) general principles, which in most cases have a rather heuristic value and may be helpful to explain common features and differences. But some of the analyzed principles may also have the potential to be applied by courts as normative standards, e.g. the exhaustion principle. It is, without any doubt, one of the most reputable tasks of European intellectual property lawyers to explore these principles and to explain their mode of operation.

**15** And, last but not least, *Miquel Peguera* would like to draw the reader's attention to

> **Reed, Chris: *Making Laws for Cyberspace*. Oxford University Press. Oxford 2012. 280 pp.**

**16** "Making Laws for Cyberspace" is an interesting and suggestive book by Chris Reed, a Professor of Electronic Commerce Law at Queen Mary, University of London, and a well-known scholar in the field of Computer and Cyberspace Law. In this book Professor

Reed explores an always challenging issue: how the laws that seek to regulate cyberspace should be devised so they can achieve their goal of influencing cyberspace actors' behaviours effectively.

**17** The question of whether cyberspace is special as to how it should be regulated is clearly answered in the affirmative. The difficult issues posed by the extraterritorially nature of the Internet and the obvious limits to meaningful enforcement suggest the need for a different approach to designing cyberspace laws. Providing an insightful analysis on the probable reasons why these laws so often fail to be accepted and obeyed by cyberspace actors, Reed proposes new ways for lawmakers to tackle this issue.

**18** The core of the argument is that cyberspace actors – whether individuals or businesses – will only abide by those laws they perceive as coming from a source with legitimate authority to regulate their actions online, and whose content appears meaningful to them. Thus, lawmakers need to ensure both elements if their laws are to be considered worthy of respect. Devising the laws from this standpoint represents a fundamental change in the normal process of law-making.

**19** When considering the authority cyberspace laws need to achieve in order to be generally accepted, Reed refers to a number of factors that may weight against them from the users' standpoint. These include users' realization that the state asserting the applicability of a particular law lacks jurisdiction over their actions online or that the law is unenforceable in practice against those users; ignorance of foreign laws, which is inevitable in cyberspace; the impossibility to comply with all the – often contradictory – laws that claim to apply to the same activity; or the users' perception that the connection between their online activities and the state that tries to assert authority on them is too weak.

**20** Professor Reed contends that the main reason why people ultimately comply with the laws in cyberspace is neither the mere applicability of the law nor the fear of enforcement. Rather, other sources of authority are taken into account by cyberspace actors, which would explain for instance the phenomenon of voluntary compliance by subjects that are not legally bound by a particular set of laws that they nonetheless accept – a conduct the author terms the "Amazon Paradox," referring to the example of the companies behind the website amazon.co.uk, which in spite of not being UK entities, abide by some UK laws not applicable to them. Among those sources of authority, the sense of community membership turns up to be of the utmost importance, especially in the case of e-commerce businesses dealing with foreign costumers.

**21** In Reed's view, cyberspace actors choose, however unconsciously, which subset of foreign rules they are prepared to accept and recognize as respect-worthy, and they do so in a rational way. However, these subsets may not necessarily coincide with the legal system of a particular state. Rather, they may be rules of other kinds of communities; based on contractual relationships, such as those resulting from ICANN's Uniform Domain Name Dispute Resolution Policy; or the rules that govern the eBay global community.

**22** The author warns lawmakers against over-asserting their authority over foreign actors and suggests targeting, instead, those who actually intend to become at least temporary members of the lawmaker's community. He underscores, as well, that it will be very difficult for a law to impose an obligation worthy of respect if that obligation clashes with a well-established norm in the relevant community – an opposition that may account for much of the failure experienced by copyright enforcement laws in cyberspace. Reed elaborates on many other aspects with regards to the content of cyberspace laws, touching upon issues such as over-complexity, contradictory rules, regulation by proxies, or wrong assumptions as to how actors are actually using cyberspace. He notes, for instance, the unintended effects that arise from embedding inappropriate business or activity models in the law. Other key aspects such as limiting the purpose of laws to achievable aims, or dealing with the rapid changes in technology are also considered.

**23** The book is well-written, reveals a thorough revision of the extensive literature in this field, and provides useful insights on how to deal with the limits of the law as a mechanism for regulating cyberspace. It will surely be a profitable read for both academics and lawmakers and will reopen the debate on these demanding issues.

■

* The first text has been prepared with the help of Nicole Fallert, Research Assistant at the Institute of Information and Economic Law, Karlsruhe Institute of Technology (KIT), Karlsruhe, Germany.

1 A recent German project on the creation of an "Allgemeiner Teil" for the various intellectual property acts has been finalized and published in 2012, see Ahrens/McGuire, Modellgesetz für Geistiges Eigentum, Sellier European Law Publisher 2012, 844 pp.

JIPITEC

Journal of
Intellectual Property,
Information Technology,
and Electronic Commerce
Law

www.jipitec.eu