

Patents and trade secrets in the internet age

DE WERRA, Jacques

Reference

DE WERRA, Jacques. Patents and trade secrets in the internet age. *Revue de droit suisse*, 2015, vol. 134. Halbbd. 2, Sonderheft, p. 123-190

DOI : 10.2139/ssrn.2684616

Available at:

<http://archive-ouverte.unige.ch/unige:75611>

Disclaimer: layout of this document may differ from the published version.



**UNIVERSITÉ
DE GENÈVE**

Patents and Trade Secrets in the Internet Age

JACQUES DE WERRA*

* The author gratefully acknowledges the assistance of Pierre Heuzé for the finalization of this report.

Contents

A.	Introduction	126
B.	Patents	127
	I. Conditions of patent protection	127
	1. Novelty	128
	a. Novelty and online existence and availability of documents	129
	b. Novelty and restricted access to online content	135
	c. Non-prejudicial disclosure as a result of an evident abuse in the online environment	136
	2. Non-obviousness and big data	142
	3. Conclusion	145
	II. FRAND patent licensing	146
	1. Introduction	146
	2. The legal nature of the commitments made by owners of SEPs	149
	3. The content of FRAND licenses	153
	4. FRAND dispute resolution mechanisms	156
	5. Conclusion	162
C.	Trade Secrets	164
	I. Introduction	164
	II. Art. 39 TRIPS	167
	1. Introduction	167
	2. Conditions of protection	169
	a. Definition of undisclosed information	169
	aa. Secrecy	169
	bb. Information which has commercial value because it is secret	174
	cc. Reasonable steps to keep the information secret	175
	b. Prohibited acts	178
	c. Balance between employee mobility and corporate trade secrets	180
	III. Conclusion	184
D.	Lessons and perspectives	184

A. Introduction

«[d]ata is at the centre of the future knowledge economy and society»¹. Accessing, using and managing online information and data have become key aspects of our professional and personal daily life. More generally, the global availability and searchability of exponentially growing amounts of data, which is made possible by continuously developing information and communication technologies (ICT), characterize but also challenge the functioning of today's society as a whole. It also questions our legal systems. While the information age obviously affects many diverse facets of the law, this report will (modestly) expose selected aspects of this transversal issue from the perspective of the law of patents and of trade secrets².

In this respect, the information age seems to be characterized by two opposite trends: one pushing towards a broader accessibility and processing of online data and resources (in terms of open data and big data³) and the other pushing for more control over digital information in the face of growing risks of online data breaches (that can materialize in cyber-attacks and in cyber-security risks, which can affect all companies in all sectors⁴).

From this perspective, the goal of this paper will particularly be to assess the impact on patent law and on trade secrets law of this facilitated accessibility and processing of online data and resources, and the impact of the risk of online data breaches. It will discuss whether the new technological environment offers an opportunity or even make it necessary to revisit and to adapt

-
- 1 Communication from the European Commission, Towards a thriving data-driven economy, July 2, 2014, COM (2014) 442 final, p. 4, available at: <http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?action=display&doc_id=6210>.
 - 2 The analysis cannot be conducted exclusively or even essentially on the basis of Swiss intellectual property law, because the issues are essentially global and because other legal systems (particularly the US system) offer quite valuable and even unique experiences and hindsight and mirror the pioneering and leading role of certain markets (specifically the US market) in the ICT industries, which is also reflected in their regulatory and judiciary activity. These foreign legal sources are of major relevance from a Swiss perspective because the legal issues ultimately arise in similar terms (though not always identical).
 - 3 This paper will not attempt to give a precise definition of these concepts (or buzz words), but will rather use them as general reference to the respective acts of increasing access to data (open data) and of processing data (big data); big data can impact IP in multiple ways; for a risk/value perspective, see NIGEL SWYCHER, Big data solutions to determining IP risk and value, Intellectual Asset Management, July/August 2014, p. 41–46.
 - 4 As recently evidenced by the highly mediatized cyberattacks on Sony in connection with the release of the movie «The Interview» in November 2014 (with potential connections with North Korea) and on TV5 Monde in April 2015; see, for the Sony attack: <<http://www.nbcnews.com/storyline/sony-hack>> and <<https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/>> and, for the TV5 Monde attack: <<http://www.bbc.co.uk/newsbeat/article/32242553/tv5monde-cyber-attack-on-a-different-scale-says-terrorism-expert>>; this report will not analyze the issues of online privacy, data protection and cyber surveillance, even if they can in various ways be closely related to the topics that shall be analyzed here.

certain concepts and principles of patent law and of trade secrets law. It will also discuss FRAND licensing which constitutes a very important – though potentially less visible – component of our information age because the availability of online information also depends on our ability (as Internet users) to use connected devices (mobile devices), which in turn presupposes the availability of patented technologies for manufacturing and commercializing such devices under fair, reasonable and non-discriminatory (FRAND) terms and conditions.

B. Patents

The information age creates many challenges for the patent law system. The choice was made here to analyze a selection of them⁵ by focusing on the main substantive conditions of patent protection (see below I) before turning to FRAND licensing (see below II).

I. Conditions of patent protection

The information age and the era of big data mean that more and more information is becoming publicly available. This in turn means, from a patent law perspective, that more and more information and documents can be part of the state of the art which may have an impact on both the standard of novelty (see below 1) as well as on the standard of non-obviousness (see below 2).

5 This report will not analyze the issue of whether and under what conditions certain inventions relating to ICT (and specifically computer software – which would be a topic by itself) can potentially be protected under patent law. As a result, no legal analysis of the protection of big data technologies by patent law (or by other intellectual property rights) will be conducted in this report; on this issue, see the interesting report of the United Kingdom Patent Office, *Eight Great Technologies; Big Data, A patent overview*, 2014 (which maps the players and trends on the patenting market for «big data and efficient computing» technologies) available at: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/325024/informatics-bigdata.pdf>; this report will not analyze either the IP challenges (and specifically the patent-related challenges) raised by 3D printing technologies, see PREETA REDDY, *The Legal Dimension of 3D Printing: Analyzing Secondary Liability in Additive Layer Manufacturing*, 16 *Columbia Science & Technology Law Review* (2014), p. 222–247, available at: <<http://stlr.org/the-legal-dimension-of-3d-printing-analyzing-secondary-liability-in-additive-layer-manufacturing/>>; DAVIS DOHERTY, *Downloading Infringement: Patent Law as a Roadblock to the 3D Printing Revolution*, *Harvard Journal of Law & Technology*, Vol. 26, Number 1 Fall 2012, p. 353–373, available at: <<http://jolt.law.harvard.edu/articles/pdf/v26/26HarvJLTech353.pdf>>.

1. Novelty

Pursuant to Art. 1 para. 1 of the Swiss Patent Act⁶, «[p]atents for inventions are granted for new inventions applicable in industry»⁷. The assessment of the novelty must be made by reference to the state of the art, which is defined, according to Art. 7 para. 2 SPA, as comprising «everything made available to the public by means of a written or oral description, by use, or in any other way prior to the filing or priority date»⁸.

According to certain sources, the condition of novelty will be increasingly difficult to meet given the exponential availability of information which shall be part of the state of the art⁹. It however remains that the condition of novelty of an invention will not be met (and the novelty will be destroyed) only if all the characteristics of the invention are found in one single item of prior art (i.e. in one single anteriority)¹⁰, which may not necessarily be easy to show given the constantly growing pool of available resources and the difficulties that may remain to locate them¹¹ (in spite of ever improving data searching and mining technologies).

One challenging issue is the relevance of online information and documents in the assessment of the condition of novelty. A reference to official patent guidelines (specifically the Guidelines for Examination in the European Patent Office¹² and the PCT International Search and Preliminary Examination Guide-

6 Swiss Federal Act on Patents for Inventions of June 25, 1954 (Swiss Patents Act, hereafter: «SPA»), available at: <<http://www.admin.ch/opc/en/classified-compilation/19540108/>>.

7 English translation available at: <<http://www.admin.ch/opc/en/classified-compilation/19540108/index.html>>; whereby this source indicates that the English translation «is provided for information purposes only and has no legal force».

8 See also Art. 54 of the Convention on the Grant of European Patents (European Patent Convention) of 5 October 1973 as revised by the Act revising Art. 63 EPC of 17 December 1991 and the Act revising the EPC of 29 November 2000 (hereafter: «EPC»):

«(1) An invention shall be considered to be new if it does not form part of the state of the art.
(2) The state of the art shall be held to comprise everything made available to the public by means of a written or oral description, by use, or in any other way, before the date of filing of the European patent application».

9 JOREN DE WACHTER, Intellectual Property in an Age of Big Data, an Exercise in Futility?, An examination of Big Data's impact on patents and database protection, CRI 1/2014, p. 1–7, at 3; see also <<http://jorendewachter.com/2013/11/big-data-ip-business-strategy/>> (analyzing the impact of big data on the conditions of patentability essentially from the perspective of novelty); for an analysis of new methods of disclosure of prior art, see ALEXANDER KLICZNIK, *Neuartige Offenbarungsmittel des Standes der Technik im Patentrecht*, Cologne 2007.

10 Swiss Federal Supreme Court, decision 4A_142/2014 of October 2, 2014, para. 6 (published in *Revue du droit de la propriété intellectuelle, de l'information et de la concurrence*, sic!, 2015, p. 49).

11 See ROLF H. WEBER, Big Data: Rechtliche Perspektiven, in: Rolf H. Weber/Florent Thouvenin (ed.), *Big Data und Datenschutz – Gegenseitige Herausforderungen*, Zurich 2014, p. 17–29, p. 23.

12 Part. G on Patentability (November 2014 ed., «the EPO Guidelines»); available at: <<https://www.epo.org/law-practice/legal-texts/guidelines.html>>; see: <[http://documents.epo.org/projects/baby_lon/eponet.nsf/0/56911A5DDF284B55C1257D81005FA359/\\$FILE/guidelines_for_examination_2014_part_g_en.pdf](http://documents.epo.org/projects/baby_lon/eponet.nsf/0/56911A5DDF284B55C1257D81005FA359/$FILE/guidelines_for_examination_2014_part_g_en.pdf)>, para. 7.5; see also the Notice from the European Patent Office concern-

lines¹³) can be useful as they contain specific rules on Internet disclosures. The EPO Guidelines confirm that disclosures of information on the Internet form part of the state of the art and adequately emphasize that certain information are actually made available only on the Internet¹⁴. The PCT Guidelines further indicate that prior art disclosure on the Internet shall be considered in the same way as other forms of written disclosure¹⁵.

a. Novelty and online existence and availability of documents

Beyond these general statements, the question arises as to what extent and under what conditions online sources can be relied upon for showing a lack of novelty. According to an interesting decision of a Board of Appeal of the European Patent Office¹⁶, the mere existence of certain prior art documents on the Internet (World Wide Web) is not sufficient for admitting that they have been made available to the public¹⁷. It is rather required to establish that «direct and unambiguous access to it by known means and methods is possible»¹⁸. On this basis, «[u]ntil it is established that such direct and unambiguous access by known means and methods was possible before the filing date, the access remains only theoretical and therefore does not meet the requirement of «made available to the public» within the meaning of Art. 54(2) EPC 1973»¹⁹. The decision further explored whether «direct and unambiguous access» was possible on the basis of the Uniform Resource Locator (URL) of the relevant web-pages (disclosing prior art). In that scenario (which can be referred to as «direct

ning internet citations, Official Journal EPO August-September 2009, Year 32, number 8–9, p. 456–462 (available at: <http://archive.epo.org/epo/pubs/oj009/08_09/08_4569.pdf>).

13 Guidelines for the Processing by International Searching and Preliminary Examining Authorities of International Applications Under the Patent Cooperation Treaty as in force from July 1, 2014 («the PCT Guidelines», available at: <<http://www.wipo.int/pct/en/texts/pdf/ispe.pdf>>; while the PCT Guidelines (as referring to the international search and the preliminary examination do not have any final impact on the assessment of the substantive validity of a patent (particularly in terms of its novelty), they are nevertheless of interest for the purpose of this discussion to the extent that they establish conditions for the relevance of Internet disclosures (their relevance was also confirmed in the decision of the Boards of Appeal of the European Patent Office, case T 1134/06 – 3.2.04, para. 3.4).

14 EPO Guidelines (note 12), para. 7.5.

15 PCT Guidelines (note 13), para. 11.13.

16 Decision T 1553/06 (Public availability of documents on the World Wide Web/PHILIPS) of March 12, 2012, available at: <<http://www.epo.org/law-practice/case-law-appeals/recent/t061553eu1.html>>.

17 Decision T 1553/06 (note 16), para. 6.5.4; some commentators seem to be more liberal and consider that the presence of prior art on the Internet can already be sufficient in order to destroy novelty, irrespective of whether users do effectively access the relevant websites, see PETER HEINRICH, PatG/EPÜ, 2nd ed., Zurich 2010, N 40 ad art. 7 («Der Umstand, dass das Internet unübersichtlich ist und dass manche Netzinhalte bzw. Websites kaum je aufgerufen werden, dürfte für die patentrechtliche Neuheit keine Rolle spielen»); see however WOLFGANG NIEDLICH, Veröffentlichungen im Internet, Mitteilungen der deutschen Patentanwälte 2004, p. 349–351.

18 *Ibid.*

19 Decision T 1553/06 (note 16), para. 6.5.5.

accessibility»), the relevant URL was relatively complex²⁰ so that the Board did not consider that it was «straightforward for a member of the public, even one with IT skills, to guess»²¹ that URL. The Board however did not exclude that in exceptional cases certain URLs would be so straightforward and so predictable «that they could readily be guessed exactly and thus be regarded as providing direct and unambiguous access to the webpages at these URLs»²². It seems however quite unlikely that such exceptional circumstances can materialize (i.e. it is hard to imagine what URL could be so simple as to be so easy to guess).

This decision further discusses the impact of the use of search engines on the accessibility of the relevant documents (such a scenario could be referred to as «indirect accessibility»). The Board stated in this respect that «the fact that a document stored on the World Wide Web could be found by entering keywords in a public web search engine before the priority or filing date of the patent or patent application, is not always sufficient for reaching the conclusion that «direct and unambiguous access» to the document was possible»²³. It however established a two prong test according to which a document available on the World Wide Web and accessible via a specific URL can be deemed to have been made available to the public, provided that the relevant document:

«(1) could be found with the help of a public web search engine by using one or more keywords all related to the essence of the content of that document and

(2) remained accessible at that URL for a period of time long enough for a member of the public, i.e. someone under no obligation to keep the content of the document secret, to have direct and unambiguous access to the document»²⁴.

The first condition relates to the way in which the content of the document can be identified by the search engine tools and technologies (whereby the terminology used by the Board in the decision referring to «the essence of the content» of the document is not crystal-clear). This condition means that if the content of the document is not adequately identified (for instance by using relevant metatags of the website or other identifiers and key words relevant to the content of the document), a search made in a search engine by key words will not be in a position to reveal the document²⁵.

The second condition reflects the transient nature of the Internet. The decision indicates in this respect that it is a «necessary condition that a document

²⁰ The URL was: <http://www.gironet.nl/home/morozov/CIE/DISPLAY_DEVICE>.

²¹ Decision T 1553/06 (note 16), para. 6.6.

²² *Ibid.*

²³ Decision T 1553/06 (note 16), para. 6.7.3.

²⁴ Decision T 1553/06 (note 16), para 6.7.3.

²⁵ The decision (note 16, para. 6.7.3.) gives the hypothetical counter-example of a document which is identified only by an arbitrary string of characters («lk8zhd94j87hir»), which would not disclose the content of the relevant document because unless the user of the search engine enters exactly that string of characters, the document will not be revealed by the search.

stored at a given URL on the Web remain accessible there for a sufficiently long period of time. Indeed, too short a period of time would effectively make it impossible to access the document. The minimum amount of time required for allowing direct and unambiguous access by a member of the public to a document must be assessed on a case-by-case basis, taking into account all the circumstances of the case»²⁶. Interestingly (and somehow surprisingly), the decision did not at all discuss the question of the (automatic) reproduction of the content of the relevant website at other online locations (mirror websites/caching mechanisms/archiving websites²⁷) which may render moot the discussion about the period of time of availability of the document at its *original* online location (i.e. at the original URL)²⁸, given that the document would remain available at other online locations.

The question also arises as to the reliability of online sources, which is particularly important for the purpose of defining the date of online publication²⁹. In this respect, the PCT Guidelines make the distinction between two types of Internet disclosure, i.e. «those made on the website of trusted publishers and those made on websites of unknown reliability»³⁰. The first category of websites, about which the PCT Guidelines indicate that online scientific publications as well as the websites of traditional media (newspapers, periodicals, television and radio stations) will «usually fall into this category as well»³¹, is characterized by the fact that the relevant websites indicate the date of online publication/disclosure, which can thus be taken into account, absent evidence to the contrary³². By contrast, for the second category of websites, the date of publication is more uncertain, whereby the PCT Guidelines list examples of such websites as including «those belonging to private individuals, private organizations (for example, clubs), commercial web sites (for example, advertis-

26 Decision T 1553/06 (note 16), para. 6.7.3.

27 It can be noted that automatic online archiving tools (specifically the Internet Archive Wayback Machine, <<https://archive.org>>) was discussed and relied upon in another decision, see Decision of the Boards of Appeal of the European Patent Office, case T 0286/10 (Sécurisation d'un accès à une ressource numérique/BOUYGUES) of May 21, 2014, available at: <<http://www.epo.org/law-practice/case-law-appeals/recent/t100286fu1.html#q>>; see also the PCT Guidelines (note 13), para. 11.17 (c).

28 The decision left open the issue as to whether the availability of the document during less than twenty minutes was sufficient in this respect (see para. 6.7.5); the view is expressed in the legal literature that one hour could as a matter of principle be considered as sufficient (whereby this period of time must be adapted to the circumstances of the case), see HEINRICH (note 17), N 41 ad art. 7.

29 See ANTOINE SCHEUCHZER, in: Jacques de Werra/Philippe Gilliéron (ed.), *Commentaire romand propriété intellectuelle*, Basel 2013, N 13 ad art. 7 LBI (noting that the date of online publication can require further investigations); see EPO Guidelines (note 12), para. 7.5.1.

30 PCT Guidelines (note 13), para. 11.13; by contrast, the EPO Guidelines (note 12) do not operate such binary distinction but at least partly refer to similar and sometimes identical standards for determining the date of publication of online sources, see para. 7.5.3.1 et seq.

31 PCT Guidelines (note 13), para. 11.14.

32 *Ibid.*

ing)»³³. The PCT Guidelines therefore suggest that the relevant authorities (i.e. the «International Searching and Preliminary Examining Authorities») shall use the following methods for establishing the publication date: (a) research the hidden date of the relevant webpage³⁴, (b) refer to the «indexing dates given to the web page by search engines»³⁵ (which are «usually later than the actual publication date of the disclosure since the search engines usually take some time to index a new web site»³⁶), or (c) refer to the «information available relating to the web site on commercial Internet archiving databases (for example, the «Internet Archive Wayback Machine»)»³⁷.

It is however not possible to trust without restriction the informational output processed by these sources (and specifically those processed by search engines). This was confirmed by a recent decision of a Board of Appeal of the European Patent Office³⁸. In this case, the Board of Appeal set aside a decision of the Examining Division which had refused the patent application at issue (for lack of inventive step³⁹) based on a prior online publication (a scientific proposal submitted for a meeting that took place in Lancaster, UK, in February 1999), which was available⁴⁰ on a scientific publication online archive (i.e. «CiteSeerX»⁴¹) and which was found by the Examining Division to have been publicly available based on a screenshot of Google search results before the relevant priority date of July 3, 1999 (of the patent application at issue). In the appeal proceedings, the appellants/applicants (Columbia University and IBM) submitted the arguments and supporting documents by which they established that the CiteSeerX database had not been in use until 2008⁴² so that the availability of the allegedly prior art document on this data-

33 PCT Guidelines (note 13), para. 11.16.

34 PCT Guidelines (note 13), para. 11.17 (a) (stating that «date information is sometimes hidden in the programming used to create the web site, but is not visible in the web page as it appears in the browser»).

35 PCT Guidelines (note 13), para. 11.17 (b).

36 *Ibid.*

37 PCT Guidelines (note 13), para. 11.17 (c).

38 Decision T 1961/13 (Audio visual data signal description/COLUMBIA UNIVERSITY) of September 16, 2014 available at: <<http://www.epo.org/law-practice/case-law-appeals/recent/t131961eu1.html>>.

39 The fact that this case was about inventive step and not about novelty (which is discussed here) is of no impact because this case more fundamentally discusses the legal relevance of online sources and online localization tools.

40 «Proposal Id: P480 Proposal for MPEG-7 Image Description Scheme», available at: <<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.30.4535&rep=rep1&type=pdf>>.

41 <<http://citeseerx.ist.psu.edu/index>>, which is a scientific literature digital library and search engine focusing primarily on the literature in computer and information science and which is hosted at the College of Information Sciences and Technology of the Pennsylvania State University (available at: <<http://ist.psu.edu/>>).

42 Interestingly, the appellants referred to Wikipedia for establishing that the CiteSeerX database was not in use before 2008 (they referred to the Wikipedia entry/website: <<http://en.wikipedia.org/wiki/CiteSeer#CiteSeerX>>, see decision, para. 3.3) which was accepted by the Board of Appeal, who did not question the relevance and reliability of this source, even if it seems reason-

base could not establish that the document was available already in 1999 (i.e. at a time when the database was not available). They also indicated that the inspection of the PDF document that was identified by the Examining Division (as being available on the CiteSeerX database) revealed that its creation date was July 25, 1999 so that this document did not establish that such PDF document existed already in February 1999 (whereby the priority date of the patent was July 3, 1999)⁴³.

They further established that the date shown in the Google search result, which was «15 Feb. 1999», did not necessarily indicate that this was the date of indexing, i.e. this date did not show that the relevant document was available and retrievable on Google on that date, contrary to what the Examining Division held by considering that the document had been a «snapshot» by Google on February 15, 1999 (which predated the priority date of the relevant patent application). The applicants indeed managed to show that the date associated with the Google search which had been relied upon by the Examining Division was not the date of indexing, by submitting another hypothetical Google search for the phrase «information superhighway» that was filtered by a date range ending on December 1, 1992. That search showed that one search result (i.e. one document) referred to a date of «September 15, 1977»⁴⁴. However, as duly acknowledged by the Board of Appeal, this date of September 15, 1977 obviously could not be the date from which the relevant document was made available on the Internet or the date at which the document was retrievable by the Google search engine (none of which existed back in 1977). On this basis, the Board of Appeal held that «a date reported by Google is inherently unsuitable to serve as evidence of the publication date of a document»⁴⁵. It further noted «that it should not have been necessary for the appellants to investigate the relevance of Google's date indications. It is the task of the examiner to make an objective assessment of what a particular date indication is intended to represent and how reliable it is, and to make further investigations if necessary. If it is not understood how a particular date reported by a search engine was generated, it cannot be used as evidence of a publication date»⁴⁶. It consequently results from this decision that the relevance and reliability of all online sources must be carefully assessed in the light of the relevant circumstances of the case and of the specificities of the sources at issue.

nable to be quite cautious about whether Wikipedia (in view of its open and evolving nature) can constitute a trustworthy online source of information, specifically for patent disclosure purposes.

43 Decision T 1961/13 (note 38), para. 3.3.

44 Decision T 1961/13 (note 38), para. 5.1.2 and 5.1.3.

45 Decision T 1961/13 (note 38), para. 5.1.5.

46 Decision T 1961/13 (note 38), para. 5.1.6.

The issue of the date of an online publication was also debated in a recent New Zealand case (*Quirky, Inc v Hamish Dobbie*⁴⁷), in which the opponent (in patent opposition proceedings) opposed the patent application on the basis that the applicant had disclosed the invention on its own crowdsourcing website⁴⁸, before the earliest priority date of the patent application. The relevant webpage provided by the opponent related to the timeline of development of the invention covered by the patent (i.e. an egg-yolk separated product referred to as «*Pluck*») using the Quirky Inc. crowdsourcing platform. The website stated that the Pluck product was first «*on sale*» on 14 December 2012. It also stated that «*on Sep 05, 2012, staff and community members joined together at Quirky HQ in New York to select Pluck to become a Quirky Invention*» and provided a video recording of this event. The decision rendered by the patent office declined to consider the Internet document provided as anticipatory evidence, because there was no evidence of the date on which the document allegedly disclosing the invention had been made available on the Internet. This case confirms that the mere availability of a piece of information on the Internet may not be sufficient and legally relevant unless all requested indications can be duly established (including the date of its online availability).

While case law is still evolving, guidelines will need to be progressively adapted and fine-tuned for assessing the relevance and reliability of online sources for patent disclosure purposes. It seems in any case important to admit that the burden of proof should, as a matter of principle, not be excessively high for Internet online disclosures by comparison to offline disclosures⁴⁹. In a world

47 *Quirky, Inc v Hamish Dobbie* [2014] NZIPOPAT 6 (14 February 2014), available at: <<http://www.nzlii.org/nz/cases/NZIPOPAT/2014/6.html>>; for a short comment, see VICTORIA M. LONGSHAW/ELIZABETH E. HOULIHAN, *It's no yolk: the dangers of using webpages as anticipatory evidence in New Zealand patent oppositions* (February 25, 2014), available at: <<http://documents.lexology.com/cc8af511-2491-417a-b590-cda2211b8bd7.pdf>>.

48 <<http://www.quirky.com/products/426-Pluck-egg-yolk-separator/timeline>>.

49 In this sense, the decision of a Board of Appeal of the European Patent Office in the case T 0286/10 (note 27) (*Sécurisation d'un accès à une ressource numérique/BOUYGUES*) of May 21, 2014 can be viewed positively, available at: <<http://www.epo.org/law-practice/case-law-appeals/recent/t100286fu1.html#q>>, see para. 2.3: «En d'autres termes les publications Internet n'impliquent pas par principe une [sic] régime dérogatoire de preuve, les incertitudes liées à ces divulgations doivent être levées de façon à procurer un degré de probabilité suffisant, et établir la présomption d'accessibilité qui emportera la conviction du juge. Il n'y a aucune raison de hausser le degré des probabilités à hauteur de l'absence de tout doute raisonnable» and para. 4.1–4.3: «La chambre en partie pour les raisons ci-dessus exposées, ne partage pas la conclusion de la décision T 1134/06 que, par principe, les archives Internet ne sont pas fiables. En particulier, la chambre considère que normalement le fait qu'un document a été archivé par l'archive Internet <<http://www.archive.org>> à une certaine date, sauf bien entendu circonstance particulière jetant une suspicion, constitue en soi une présomption suffisante que le document a été accessible au public au jour de téléchargement et, rendu accessible au public via l'archive Internet elle-même peu après.

4.2 L'archive Internet, une initiative d'archivage privé et non-lucratif (voir aussi T 1134/06, motifs 3.2), met à la disposition du grand public d'instantanés antérieurs de l'Internet. Depuis sa création in [sic] 1996, elle est devenu [sic] très populaire et a développé une bonne réputation.

which is moving online and in which online information will progressively replace or at least largely outpace offline information sources, it would be inadequate to block and oppose such evolution by still giving more evidentiary weight to offline publications and actions by comparison to online sources. In other words, the old economy (brick and mortar, B&M) and publishing (books and magazines, also B&M) models should not remain the guiding references in an era of online business and publications.

b. Novelty and restricted access to online content

The EPO Guidelines further provide that «[n]either restricting access to a limited circle of people (e.g. by password protection) nor requiring payment for access (analogous to purchasing a book or subscribing to a journal) prevent a web page from forming part of the state of the art. It is sufficient if the web page is in principle available without any bar of confidentiality»⁵⁰. It however appears uncertain to consider categorically that «restricting access to a limited circle of people (e.g. by password protection)» will not prevent «a web page from forming part of the state of the art». This seems to neglect that the access to a given webpage could be restricted to only certain people (potentially from inside the relevant company – having filed the patent application) and that the technological access protection mechanisms can ensure that people having access are bound by a (contractual) obligation of confidentiality⁵¹. In such a case, it appears quite restrictive to consider that such technological access protection mechanisms would not help preserve the confidentiality of the relevant web page (i.e. the information made available on such web page) so that such information would form part of the state of the art and be considered to be available to the public.

Même si le volume de données traitées est énorme, l'archive n'est, naturellement, qu'une collection incomplète des pages Internet antérieures. Cependant, des bibliothèques classiques sont incomplètes elles aussi sans affecter la crédibilité de l'information disponible. Bien que la chambre ne nie pas que des doutes sur les entrées individuelles dans l'archive Internet puissent surgir, elle estime que l'archive elle-même présente des garanties suffisantes pour bénéficier d'une présomption de source d'information fiable et de confiance, à charge pour la partie adverse de produire, en fonction de l'espèce, les éléments de nature à jeter un doute sur cette fiabilité présumée et par là même détruire cette présomption.

4.3 Pour cette raison, il ne saurait suffire à l'intimée de se borner à invoquer en général un manque de fiabilité de l'archive Internet pour mettre en doute la date d'accessibilité publique d'un document archivé sur <<http://www.archive.org>>; for a restrictive view, see the decision of the German Bundespatentgericht, ref. BPatG 17W (pat) 1/02, GRUR 2003, p. 323, confirmed by BPatG 17W (pat) 47/00 (ruling that the Internet was not a reliable source for determining the state of the art).

50 See the EPO Guidelines (note 12), para. 7.5.1 (which bears the title: «Establishing the publication date»).

51 Whereby such obligation of confidentiality can result either from a preexisting contract (such as an employment contract), or from the contract that those accessing the protected content online would have to accept in order to gain access (in the form of a click through agreement), whereby the validity of such an agreement should also be established.

Interestingly, a recent decision of a Board of Appeal of the European Patent Office indicated that the situation in which access to a document is protected by a password is similar to the one in which the public has to guess an URL in order to access a webpage, in which case it held that guessing the relevant URL did not provide direct and unambiguous access and thus did not make the relevant documents available to the public so that the novelty was maintained⁵².

c. Non-prejudicial disclosure as a result of an evident abuse in the online environment

Another question which must be addressed is whether a cyber-attack on a given website (by which unauthorized access to a piece of confidential information covered by a patent application would have been obtained and following which such information would be made available online) could constitute a non-prejudicial disclosure because such disclosure would be due to «an evident abuse in relation to the applicant»⁵³. If it were the case, this would mean that such disclosure of the relevant information would not be prejudicial to the validity of the patent (i.e. it would not bar the finding that the condition of novelty would be met). Based on the EPO Guidelines⁵⁴, an evident abuse implies either an actual intent to cause harm to the patent applicant, or an actual or a constructive knowledge that harm could result from such disclosure⁵⁵.

According to a decision of a Board of Appeal of the European Patent Office⁵⁶, a finding of an evident abuse implies a breach of an obligation of confi-

52 See Decision T 1553/06 (note 16) (Public availability of documents on the World Wide Web/ PHILIPS) of March 12, 2012, available at: <<http://www.epo.org/law-practice/case-law-appeals/recent/t061553eu1.html>>.

53 See Art. 7b SPA (Non-prejudicial disclosures): «Where the invention has been made available to the public in the six months prior to the application date or priority date, this disclosure does not form part of the state of the art when it is due to, or a consequence of: a. an evident abuse in relation to the patent applicant or his legal predecessor [...]»; see also art. 55 EPC para. 1: «For the application of Article 54, a disclosure of the invention shall not be taken into consideration if it occurred no earlier than six months preceding the filing of the European patent application and if it was due to, or in consequence of: (a) an evident abuse in relation to the applicant or his legal predecessor [...]»; it can be noted that the differences between the solution of Art. 7b SPA and Art. 55 EPC have been criticized in the recent legal literature and that proposals have been suggested to bring the Swiss regulation in line with the European one (specifically with respect to the starting point of the grace period): see SIMON STRÄSSLE/MICHAEL LIEBETANZ, *Schonzeit für ältere Rechte in der Schweiz*, sic! 2013, p. 428 (this issue is however not of particular relevance for the discussion here).

54 See above note 12.

55 See the EPO Guidelines (note 12), Chap. V, para. 3: «For «evident abuse» to be established, there must be, on the part of the person disclosing the invention, either actual intent to cause harm or actual or constructive knowledge that harm would or could ensue from this disclosure (see T 585/92)»; KŁICZNIK (note 9), p. 186–187 indicates that it will be quite difficult to establish that Art. 55 EPC can apply in Internet-related contexts.

56 Decision of February 9, 1995, Case Number: T 0585/92 (Deodorant detergent/UNILEVER), para 3.3.2, available at: <<http://www.epo.org/law-practice/case-law-appeals/pdf/t920585ex1.pdf>>.

dentiality which may implicitly result from the circumstances of the disclosure or may result expressly from a formal obligation of confidentiality⁵⁷. In these cases, «the recipient of the information would know or should know the likely commercial and legal consequences of any unauthorized disclosure. Such a disclosure, made either with actual intent to cause harm (here commercial damage), or with actual knowledge (cf. constructive knowledge) that some such harm would or could reasonably be expected to result from it, would amount to an abuse in relation to the owner of the information»⁵⁸. By contrast, if the disclosure is the result of a mistake or a negligence committed by the person, this cannot constitute a case of evident abuse within the meaning of Art. 55 (a) EPC⁵⁹. In short, there can be no abuse, let alone an evident abuse, in case of mere negligence.

While these sources seem to insist on the *subjective* condition for finding an «evident abuse» (as reflected in the mindset of the abuser), they also indicate that an *objective* condition must be met: there cannot be any abuse if there is no specific relationship of confidence between the abuser and the applicant which can result from the circumstances of the disclosure or from an express agreement of confidentiality or of secrecy between the parties⁶⁰. On this basis, if there is no specific relationship of trust between the parties, there cannot be any evident abuse.

A slightly different approach seems⁶¹ to be prevalent under Swiss law which derives from the acknowledgment that the novelty of an invention shall be deemed to be preserved if the relevant information is disclosed to third parties that are bound by an obligation of confidentiality between the patent application/owner and the disclosing third party⁶². On this basis, what counts for the

57 Decision of February 9, 1995 (note 56), para. 6.5: «Normally where unauthorized disclosure of information takes place, there exists a legally enforceable obligation of confidence between the giver and the recipient of the confidential information. This confidentiality may arise from the circumstances of the disclosure or, as is more often the case, be brought about by an express confidentiality or secrecy agreement».

58 Decision of February 9, 1995 (note 56), para. 6.5.

59 Decision of February 9, 1995 (note 56), para. 6.5: «Such a disclosure made by dint of mere inadvertence or a genuine mistake, however unfortunate and detrimental its results may turn out to be, is not tainted with the necessary amount of actual or constructive knowledge and therefore guilty inadvertence so as to turn it into an evident abuse within terms of Article 55(1)(a) EPC»; in that case, the disclosure was made by mistake by the Brazilian patent office and it was stated (ibid.) that «the disclosure by the Brazilian Patent Office was a result of a «lamentable error», and lamentable errors or simple mistakes do not, as was said before, qualify as «abuse», let alone evident abuse, which is the standard of reprehensibility laid down by Art. 55(1)(a) EPC».

60 What is referred to as a «legally enforceable obligation of confidence» in the decision of February 9, 1995 (note 56), para. 6.5.

61 There is no published case law of the Swiss Federal Supreme Court or of the Federal Patent Court discussing and interpreting specifically the conditions of Art. 7b para. a SPA; for a cantonal case, see Commercial court of Berne, RSPI 1993, p. 129–138.

62 See ATF 117 II 480 para. 1c: «Massgebend ist vielmehr, dass die Erfindung trotz einer allenfalls bestehenden Geheimhaltungspflicht durch eine Benutzungshandlung offenbart worden ist, und

purpose of deciding whether a disclosure shall be non-prejudicial under Art. 7b SPA is essentially whether the legitimate expectations of confidentiality of the patent applicant/owner have been disappointed by a disclosure which has been committed by the party to which the information was disclosed, irrespective of the potential bad faith of the party disclosing the information⁶³. However, it remains debated whether a disclosure that would be made by negligence or even that would be made in good faith could result in an «evident abuse»⁶⁴.

One hypothetical scenario could result from a situation in which the patent applicant/owner would have relied on cloud-based data storage services which would have proved unsafe so that the relevant information would have leaked. In such a case, it appears doubtful that the mere negligent (involuntary) disclosure of the relevant information by the cloud service provider (as resulting from an insufficient safety system) could be viewed as constituting an «evident abuse»⁶⁵. However, if by certain maneuvers access to the relevant content could be gained by a third party intruder who would have misled the cloud service provider, this element could affect the legal outcome given that this would introduce a level of unfairness which characterizes the condition of «evident abuse»⁶⁶. It is worth emphasizing in this respect that the causality between the abusive conduct and the detrimental disclosure is relatively flexible to the extent that it is not required that there shall be an immediate link between the abusive conduct and the disclosure⁶⁷.

zwar an eine Abnehmerin, die in keinem Vertrags- oder Geschäftsverhältnis zur Klägerin stand und daher ihr gegenüber auch nicht vertraglich oder aus anderen Gründen zur Geheimhaltung verpflichtet sein konnte».

63 See HEINRICH (note 17), N 7 and 8 ad art. 7b (holding that ««Offensichtlicher Missbrauch» setzt hingegen keine boshafte oder leichtfertige Absicht desjenigen voraus, der die Erfindung aus der Sphäre des Patentinhabers an die Öffentlichkeit gebracht hat»).

64 For a discussion, see HEINRICH (note 17), N 8 ad art. 7b (who ultimately considers that good faith cannot bar a finding of abusive disclosure).

65 See Decision of February 9, 1995 (note 56), para. 6.5.

66 See Decision of February 9, 1995 (note 56), para. 6.5 (considering in that case that the behavior at issue was not «tainted with the necessary amount of actual or constructive knowledge and therefore guilty inadvertence so as to turn it into an evident abuse within terms of Art. 55(1)(a) EPC»).

67 Although this element does not seem to have been debated so far, this results from the wording of the relevant legal provisions (i.e. Art. 7b SPA and Art. 55 EPC), and specifically from their German and French versions (it being noted that, with respect to the EPC, the English, German and French official versions are equally authentic pursuant to Art. 177 para. 1 EPC). The German and French versions provide that a disclosure is irrelevant if it *directly or indirectly* originates in an evident abuse (German version: «(1) Für die Anwendung des Artikels 54 bleibt eine Offenbarung der Erfindung ausser Betracht, wenn sie [...] und *unmittelbar oder mittelbar zurückgeht*: a. auf einen offensichtlichen Missbrauch zum Nachteil des Anmelders oder seines Rechtsvorgängers [...]» (italics added); French version: «(1) Pour l'application de l'Art. 54, une divulgation de l'invention n'est pas prise en considération si [...] et si elle *résulte directement ou indirectement* [...] a) d'un abus évident à l'égard du demandeur» (italics added). This direct or indirect link of causation is not reflected with the same clarity in the English version of the EPC which provides in the relevant part that «a disclosure of the invention shall not be taken into

If the patent applicant/owner were negligent in protecting the relevant information so that such information would leak (as a result of a third party action), it is unlikely that such disclosure would qualify as a non-prejudicial disclosure because in such a case it would be difficult to admit that this disclosure would result from an «evident abuse». In other words, there shall be no finding of «evident abuse» if the patent applicant/owner acted (or potentially omitted to act) with negligence.

In this respect, an analogy could be drawn with a similar issue which arises under copyright law relating to the protection against the circumvention of technological protection measures. In such a case, the availability of legal protection against the circumvention of technical protection measures (i.e. technologies protecting against the unauthorized access or use of copyright protected content) similarly depends on the technological *efficiency* of such measures. This is reflected in Art. 11 (Obligations concerning Technological Measures) of the WIPO Copyright Treaty («WCT») which provides that «[c]ontracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of *effective technological measures* that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law»⁶⁸ (italics added). This is also adopted in the regional and national regulations which implement this provision⁶⁹. Defining what constitutes «effective technological measures» is not obvious⁷⁰. The treaty adoption history reveals that this requirement of effective

consideration if [...] it was *due to, or in consequence of*: (a) an evident abuse in relation to the applicant or his legal predecessor [...]» (italics added).

68 Art. 18 of the WIPO Performances and Phonograms Treaty (WPPT) has a similar wording.

69 For Switzerland, see Art. 39a of the Swiss Copyright Act of October 9, 1992 («SCA») which provides that:

«(1) Effective technological measures for the protection of works and other protected subject-matter may not be circumvented.

(2) Effective technological measures in accordance with paragraph 1 means technologies and devices such as access control, copy control, encryption, scrambling and other modification mechanisms that are intended and suitable for preventing or limiting the unauthorized use of works and other subject-matter»; it appears uncertain to consider that technological measures could still be viewed as «effective» even if they are «intended and suitable for *limiting* the unauthorized use» (italics added) because in such a case they would not *exclude* such use (this is also reflected in the official language versions of the legal text: German: «[...] die dazu bestimmt und geeignet sind, unerlaubte Verwendungen von Werken und anderen Schutzobjekten zu verhindern oder einzuschränken. [...]»; French: «[...] destinés et propres à empêcher ou à limiter les utilisations non autorisées d'œuvres et d'autres objets protégés [...]»; Italian: «[...] destinati e atti a impedire o limitare impieghi non autorizzati di opere e di altri oggetti protetti [...]). The mere limitation against an unauthorized use could indeed be construed as an admission of the intrinsic weakness (i.e. not circumvention-proof) of the relevant technologies (because it would not and could not *prevent* unauthorized use).

70 KAMIEL KOELMAN/NATALI HELBERGER, *Protection of Technological Measures* (Institute of Information Law ed.), Amsterdam 1998, p. 9 (stating that «what exactly constitutes an «effective» measure is unclear»).

tiveness was introduced in order to make sure that technological protection measures which could be too easily circumvented⁷¹ or which could even be circumvented «by accident» should not be legally protected (i.e. the circumvention of such measures should not be held illegal)⁷². By contrast, it is obvious that technological protection measures that would be completely efficient, in the sense that they could not be circumvented at all, do not need any additional legal protection⁷³.

The comparison between the issue under patent law (i.e. under what conditions can a piece of information available on an access-protected web site be deemed to be part of the state of the art?) and the one under copyright law (i.e. under what conditions can the unauthorized access to a copyright protected content available on an access-protected web be legally enjoined) indicate that in both cases there shall be no protection if the content at issue is not *effectively* protected against undue access. If access can be gained without excessive difficulties, no protection would be available because the piece of information at issue could be considered – under patent law – to form part of the state of the art (so that the related invention would not meet the condition of novelty) or would be viewed – under copyright law – as not having been protected by «effective» technological protection measures.

Viewed from another angle, there shall be no protection if the relevant entity (or individual) controlling the information at issue, and making it available online subject to access-control technologies, has not adopted and implemented sufficiently effective access protection technologies. The risk can particularly result from the use of remote data storage systems based on cloud computing solutions which must be adequately controlled and monitored.

The next issue relates to the definition of the standard of technological control that shall be considered as sufficient. It appears adequate to consider that *reasonable* measures shall be taken in order to prevent the unauthorized access⁷⁴ in the sense that sufficiently serious efforts should be made by the relevant entity in order to ensure that no unauthorized access shall be possible. This standard of care and diligence can however not imply that the efforts shall ensure a totally intrusion-free technological environment (which would in any case be impossible to achieve). On this basis, a legal standard based on the *reasonableness* of the measures would make it possible to adopt a flexible approach which would take into account the circumstances of the case at issue. It is worth noting that this standard could be viewed as a transdisciplinary stan-

71 ANDRÉ LUCAS, *Droit d'auteur et numérique*, Paris 1998, p. 274 («[...] le droit n'a pas à venir au secours de celui qui n'utilise même pas toutes les ressources de la technique»).

72 KOELMAN/HELBERGER (note 70), p. 9; with respect to the Swiss Copyright Act, see MICHEL JACCARD/JEROME HEUMANN, in: Jacques de Werra/Philippe Gilliéron (ed.), *Commentaire romand propriété intellectuelle*, Basel 2013, N 12–13 ad art. 39a.

73 *Universal City Studio Inc. v. Reimerdes*, 111 F. Supp. 2d 294 (S.D.N.Y. 2000), at *318.

74 Whereby the issue is to *prevent* the unauthorized access and not only to *limit* it.

dard to the extent that other regulations do also require that certain safety and security measures be taken in order to benefit from the protection (e.g. data protection laws⁷⁵ and criminal law⁷⁶).

As reflected by the California Civil Code (about personal information), the requirement is to take «reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure»⁷⁷. These measures must consequently comply with the principle of proportionality⁷⁸.

This flexibility is needed because the measures shall particularly reflect the continuous evolution of the technologies at issue. What would be considered as sufficient in year X would most certainly not be held as sufficient in year X + 1 (and even perhaps after a few months). It shall also reflect the specificities of the relevant entity/individual to which the relevant standard of conduct would apply. In this respect, it appears reasonable to take into account the size of the company: the standard of protection that can be expected from a major multinational company will not necessarily be the same as the one applicable to a local company or even to an individual, for instance an individual inventor, as well as the types of business activity and of information at issue (some industries being obviously more reliant on confidentiality than others). It will also be important to ensure that the standards of security are and remain proportionate and shall be adapted in the sense that their level of protection shall be regularly controlled and reviewed⁷⁹.

This in turn raises the issue of the potential (contractual) liability of providers of online access technologies in regards to the reliability of their technolo-

75 Reference can be made here to the «Guide relatif aux mesures techniques et organisationnelles de la protection des données» (last updated: April 11, 2014) of the Federal Data Protection and Information Commissioner (FDPIC), available at: <<http://www.edoeb.admin.ch/datenschutz/00628/00629/00636/index.html?lang=fr>>.

76 See Art. 143 para. 1 of the Swiss Criminal Code («SCC») which provides that «[a]ny person who for his own or for another's unlawful gain obtains for himself or another data that is stored or transmitted electronically or in some similar manner and which is not intended for him and *has been specially secured to prevent his access* is liable to a custodial sentence not exceeding five years or to a monetary penalty» (italics added) and Art. 143bis SCC which similarly provides that «[a]ny person who obtains unauthorized access by means of data transmission equipment to a data processing system that *has been specially secured to prevent his access* is liable on complaint to a custodial sentence not exceeding three years or to a monetary penalty» (italics added).

77 California Civil Code § 1798.81.5(b).

78 See WOLFGANG STRAUB, Cloud Verträge – Regelungsbedarf und Vorgehensweise, PJA/AJP 2014, p. 905–923, p. 912 footnote 64.

79 See STRAUB (note 78), p. 912 footnote 66, with references to other sources in the legal literature (including ASTRID EPINEY/TOBIAS FASNACHT, in: Eva Maria Belser/Astrid Epiney/Bernhard Waldmann (eds), Datenschutzrecht: Grundlagen und öffentliches Recht, Bern 2011, p. 556 para 54); according to this source, the level of security shall be reviewed on an annual basis as well as in case of important changes (specifically in case of changes of IT-system). It however appears that the frequency of such controls shall also be proportionate and shall consequently also depend on the size and complexity of the company and of the data at issue.

gies and the level of protection that they can offer against data breaches which may result in the loss of protection under patent law or other laws (specifically under the law of trade secrets)⁸⁰. It also raises the more general issue of IT corporate governance⁸¹ and of insurances for cybersecurity risks⁸².

2. *Non-obviousness and big data*

The standard of non-obviousness (or of inventive step) reflects the requirement of innovation and of creativity of the invention at issue⁸³. Pursuant to Art. 1 para. 2 SPA, «[a]nything that is obvious having regard to the state of the art (Art. 7 para. 2) is not patentable as an invention»⁸⁴. According to Art. 7 para. 2 SPA, «[t]he state of the art comprises everything made available to the public by means of a written or oral description, by use, or in any other way prior to the filing or priority date». Art. 50 para. 1 SPA also provides that «[t]he invention must be described in the patent application in such a manner that it can be carried out by a person skilled in the art».

What is of relevance here is to assess whether, and how massive data processing and analyzing tools (big data), could potentially affect the standard of non-obviousness. According to the case law of the Swiss Federal Supreme Court⁸⁵, this standard is not met and there shall consequently be no patent protection for what a person skilled in the art can logically develop on the basis of the state of the art and of an average level of expertise⁸⁶. By contrast to the condition of novelty, the assessment of the non-obviousness of an invention requires to cover

80 For trade secrets, see below C.2.a.ac (for the reasonable steps of protection that are expected in order to benefit from the protection of trade secrets); on the issue of liability, see e.g. DAN GILLMOR, *Plugging Up the Holes: Should software-makers be held liable for the Sony hack?*, December 18, 2014, available at: <http://www.slate.com/articles/technology/future_tense/2014/12/sony_pictures_entertainment_hack_should_software_makers_be_held_liable.html>; NICK HEATH, *Should developers be sued for security holes?*, August 23, 2012, available at: <<http://www.techrepublic.com/blog/european-technology/should-developers-be-sued-for-security-holes/>>.

81 ANNETTE WILLI, *IT-Governance als Aufgabe des Verwaltungsrates*, Zurich 2008.

82 On legal aspects of IT security, see ROLF H. WEBER/ANNETTE WILLI, *IT-Sicherheit und Recht: Grundlagen eines integrativen Gestaltungskonzepts*, Zurich 2006.

83 Art. 27 para. 1 TRIPS provides that «1. Subject to the provisions of paragraphs 2 and 3, patents shall be available for any inventions, whether products or processes, in all fields of technology, provided that they are new, involve an inventive step and are capable of industrial application [footnote 5]», whereby footnote 5 indicates that «[f]or the purposes of this Article, the terms «inventive step» and «capable of industrial application» may be deemed by a Member to be synonymous with the terms «non-obvious» and «useful» respectively».

84 English translation available at: <<http://www.admin.ch/opc/en/classified-compilation/19540108/index.html>>: whereby this source indicates that the English translation «is provided for information purposes only and has no legal force».

85 Which reflects a standard approach beyond Switzerland; see EPO Guidelines (note 12), Part G Chap. VII Inventive Step; PCT Guidelines (note 13), chap. 13.

86 Swiss Federal Supreme Court, decision 4A_142/2014 of October 2, 2014, sic! 2015, p. 49, (note 10), para. 7.

the state of the art in its globality. This means that all the anteriorities available to the public build together the technical background information on which the person skilled in the art (possessing standard skills to combine them) can rely in order to solve the technical problem at issue. It must consequently be assessed whether the state of the art suggests an obvious combination of different elements. It is however not possible to artificially adopt a retrospective approach which would start from the solution and would consider that the combination would obviously result from the state of the art.

The issue is thus whether increasingly sophisticated data search tools and artificial intelligence systems will affect the standard of non-obviousness and the definition of the level of knowledge that can be expected from the person skilled in the art (who can sometimes be conceived as a team)⁸⁷.

As we are moving from a world of *retrospective* software solutions for business intelligence and analytics (BIA) – in which the data are used for measurement and reporting – to *prospective* BIA software solutions which aim at developing prediction, forecasting and modeling⁸⁸, this evolution could impact the concept of non-obviousness. It must be noted that technological tools can play a significant role in patent strategies, for instance by creating massive amounts of software-generated variants of patent claims, which can then be published so that they may constitute prior art for the purpose of preventing follow-up patenting by competitors⁸⁹.

87 EPO Guideline (note 12), chapter VII.3 (stating that «[t]here may be instances where it is more appropriate to think in terms of a group of persons, e.g. a research or production team, rather than a single person (see T 164/92 and T 986/96)»; for a case discussing the composition of a «skilled team», see the UK case *Medimmune Ltd v Novartis Pharmaceuticals UK Ltd & Ors* [2012] EWCA Civ 1234 (10 October 2012); see also the Resolution of AIPPI – Question Q213 – The person skilled in the art in the context of the inventive step requirement in patent law – Paris 2010, para 4 (available at: <<https://www.aippi.org/download/committees/213/RS213English.pdf>>); on the impact of artificial intelligence on patent law (and on the standard of non-obviousness), see WILLIAM SAMORE, *Artificial Intelligence and the Patent System: Can a New Tool Render a Once Patentable Idea Obvious?*, 29 *Syracuse Science & Technology Law Reporter*, p. 113–142 (Fall 2013), available at <<http://jost.syr.edu/wp-content/uploads/Samore-Final.pdf>>.

88 See RICHARD KEMP, *Legal aspects of managing big data*, October 2014, p. 1–28, available at: <<http://www.kempitlaw.com/legal-aspects-of-managing-big-data-white-paper/>>.

89 This is the business model and software product of a French company (Cloem) which «creates, then timestamps and optionally publishes massive amounts of variants of your patent claims, called cloems™, which may be prior art (check with your patent attorney). Cloem uses proven claim drafting techniques and the best dictionaries. Trusted timestamping is used. Cloems can remain private or can be optionally published, you decide. Public cloems are searchable. Each cloem is associated with a unique and permanent address», see <<https://www.cloem.com/>>; for another use of data processing technologies in patent law, see NAOUEL KARAM/SHASHISHEKAR RAMAKRISHNA/ADRIAN PASCHKE, *Rule reasoning for legal norm validation of FSTP facts*, presented at the 1st International workshop on Artificial Intelligence and IP Law, AIIP-Jurix 2012 – Amsterdam (<<http://arxiv.org/ftp/arxiv/papers/1412/1412.3137.pdf>>) according to which: «Non-obviousness or inventive step is a general requirement for patentability in most patent law systems. An invention should be at an adequate distance beyond its prior art in order to be patented. Fulfilling a minimum measurement limit would enable a patent applicant to have its

The issue is thus whether it will not progressively be expected from a person skilled in the art to use such technological intelligent data aggregation tools which will make it possible to generate (potentially unexpected or even unpredictable) connections between these different sources and pieces of information, which could not be made and could not be expected without such tools⁹⁰. This could particularly have an impact on *combination* inventions which precisely result from innovative combinations resulting from different sources. As stated in the Case law of the EPO boards of appeal⁹¹, «in assessing the inventive step involved in an invention based on a combination of features, consideration must be given to whether or not the state of the art was such as to suggest to a skilled person precisely the combination of features claimed»⁹². This source further states that «[t]he question is not whether the skilled person, with access to the entire prior art, *could* have made the combination according to the invention, but whether he actually *would* have done so in expectation of an improvement»⁹³ (emphasis in the original document – in bold). From this perspective, it is likely that intelligent data search technologies will facilitate the processes of combination so that it shall be easier to admit that «the state of the art was such as to suggest to a skilled person precisely the combination of features claimed»⁹⁴. Big data tools and data processing technologies will indeed increasingly and *proactively* suggest creative combinations of sources rather than simply respond *passively* to data search requests⁹⁵. Online data processing tools

invention patented. Based on this fact, we proposed a method for non-obviousness analysis of a patent over its prior arts, based on highest court's precedents, called the FSTP» [i.e. Fact Screening and Transforming Processor (FSTP), which is a project funded by the Teles Pri GmbH: <<http://www.fstp-expert-system.com>>]; see also the business proposed by Aistemos (<<https://aistemos.com/>>) and its «cipher» patent analytics product which is a «data analytics solution to aggregate, analyze and visualize the world's patent, litigation and licensing data» (<<https://aistemos.com/cipher-patent-analytics/>>).

90 This is what was reflected by BEN McENIERY, *Physicality and the Information Age: a Normative Perspective on the Patent Eligibility of Non-Physical Methods*, 10 *Chicago-Kent Journal of Intellectual Property* (2010), p. 106–167 (available at: <<http://scholarship.kentlaw.iit.edu/cgi/viewcontent.cgi?article=1087&context=ckjip>>), p. 141 (with a focus on the mission of patent offices/examiners and on patents related to non-physical methods, whereby his statements can be generalized): «Advances in information management technologies can be employed by patent offices to create better, more intelligent, artificial searching tools to assist the search for prior art. *Advances in the field of artificial intelligence, data searching and legal expert systems will reach a stage where they can be reliably used by a patent examiner to determine whether an invention is actually novel and non-obvious and state what the common general knowledge in the relevant field is*» (italics added).

91 7th edition, September 2013, available at: <<http://www.epo.org/law-practice/case-law-appeals/case-law.html>>.

92 Case law of the Board of Appeal (note 91), chapter 9.2.1 Existence of a combination invention, p. 205.

93 *Ibid.* (with references to the case law of the Boards of appeal).

94 *Ibid.*

95 On the increasing innovativeness of technology tools (software) and on the impact on patent law, see in general ROBERT PLOTKIN, *The Genie in the Machine: How Computer-Automated Inventing is Revolutionizing Law and Business*, Stanford University Press 2009.

and technologies are constantly improving on the basis of the data that they receive and that they generate, as illustrated by the continuous learning processes of search engines, which can materialize – in their visible part – in their «auto-complete» function⁹⁶ (which may in turn generate legal problems⁹⁷).

The risk is also that the search of potential prior art conducted by Internet searches could itself lead to the undue disclosure of the relevant – still secret – invention which is the object of the patent application. Certain patent examination guidelines specifically address this issue by preventing such undue disclosure⁹⁸, thereby confirming that search engines gather and keep information resulting from searches that they process.

3. Conclusion

Massive online data and smart data processing can have an impact on the assessment of the substantive conditions of patent protection (i.e. the standards of patent novelty and of non-obviousness) in the sense that they question the conditions under which data can be deemed to be accessible and be part of prior art (novelty), as well as the conditions under which new *knowledge* can be deemed to be flowing (evidence – non-obviousness) from the mass of *existing* knowledge (state of the art). Smart data processing may also lead to a potential adaptation of the legal concept of the «person skilled in the art» who may at some point become a computer-assisted or data-smart person skilled in the art in the sense that it may progressively be expected that such person shall use data processing and combination technologies.

96 Such as Google auto-complete, which indicate that «[t]he search queries that you see as part of Autocomplete are a reflection of the search activity of users and the content of web pages», see: <<https://support.google.com/websearch/answer/106230?hl=en>>.

97 On this issue, see the decision of the German Bundesgerichtshof of May 14, 2013, ref. VI ZR 269/12, BGHZ 197, 213; for Switzerland, see the decision of the cantonal court of Jura of February 11, 2011 (CC 117/2010) and the comment of THOMAS WIDMER, Les «suggestions» de Google devant la justice jurassienne, *sic!* 2012, p. 126.

98 See the Manual of Patent Examining Procedure (MPEP) of the US Patent and Trademark Office (USPTO), 9th Edition, March 2014, sec. 904.02(c) Internet Searching (available at: <<http://www.uspto.gov/web/offices/pac/mpep/s904.html#d0e115787>>) referring to Art. 9 of the Patent Internet Usage Policy establishing a policy for use of the Internet by US patent examiners and other organizations within the USPTO, 64 Federal Register 33056 (June 21, 1999), (available at: <<http://www.uspto.gov/web/offices/com/sol/notices/fr990621.htm>>): «The ultimate responsibility for formulating individual search strategies lies with individual Patent Examiners, Scientific and Technical Information Center (STIC) staff, and anyone charged with protecting proprietary application data. When the Internet is used to search, browse, or retrieve information relating to a patent application which has not been published, other than a reissue application or reexamination proceeding, *Patent Organization users MUST restrict search queries to the general state of the art unless the Office has established a secure link over the Internet with a specific vendor to maintain the confidentiality of the unpublished patent application. Non-secure Internet search, browse, or retrieval activities that could disclose proprietary information directed to a specific application which has not been published, other than a reissue application or reexamination proceeding, are NOT permitted*» (italics added).

Cyber-attacks and massive data breaches also make it necessary to revisit the standard of diligence that shall be expected from the patent applicants for preventing an Internet leakage from the perspective of the conditions under which abusive online disclosures could potentially be admitted as non-prejudicial disclosures. This points to the need to adopt reasonable measures of protection and also invites to conceive a transversally coherent system between the legal standards to be imposed under patent law and other laws, including under the law of trade secrets⁹⁹: there should be a coherent approach between the finding of an invention's abusive (non-detrimental) online disclosure (to be patented) under patent law and an online misappropriation of trade secrets (as a result of a data breach) so that there shall be no abusive disclosure under patent and no misappropriation of trade secrets if the owner has not taken reasonable steps to protect its confidential information.

II. FRAND patent licensing

1. Introduction

The interaction between intellectual property law (and specifically patent law) and standardization is complex¹⁰⁰. While intellectual property law (patent law) grants exclusive rights (thereby empowering the owner of the relevant intellectual property rights to prevent any unauthorized commercial use of the protected intangible asset right), the process of standardization defines common technical standards¹⁰¹ that must be used in order for a product to comply with the relevant technological standard (for instance Wi-Fi). Standards are of essential importance in the Information and Communication Technology (ICT) industry¹⁰².

⁹⁹ As will be discussed below, see C.

¹⁰⁰ See the dedicated website: <<http://www.wipo.int/patent-law/en/developments/standards.html>>; for patents and standards, see the report Standards and Patents (doc. ref. SCP/13/2) prepared for the 13th session of WIPO's standing committee on patents (Geneva, March 23–27, 2009), available at: <http://www.wipo.int/edocs/mdocs/scp/en/scp_13/scp_13_2.pdf>.

¹⁰¹ See the definition of technical standards in the report of the International Telecommunication Union (ITU), Understanding patents, competition and standardization in an interconnected world (July 1, 2014), available at: <<http://www.itu.int/en/ITU-T/ipr/Pages/Understanding-patents,-competition-and-standardization-in-an-interconnected-world.aspx>> («the ITU Report»), p. 15: «Technical standards generally refer to the establishment of norms and requirements for technical systems, specifying standard engineering criteria, methodologies or processes. The functionality of systems incorporating communicating parts is especially dependent on conformance with common standards. Here, we often speak of «compatibility standards», also known as «interoperability standards». These standards specify how technologies such as a mobile phone and a mobile network, or a compact disc and a compact disc player, interact with one another and work together successfully. Compatibility and interoperability standards are most common in the ICT and consumer electronics sectors, but their importance to other industry sectors is growing rapidly».

¹⁰² See ITU Report (note 101), p. 23, with a chart listing examples of international SSOs and consortia and their standards of relevance to ICTs.

Technical standards integrate patented technologies owned by a wide range of companies, which thus become «standard essential patents» (SEPs)¹⁰³, in the sense that any company wishing to use and implement the relevant standards in its products (which is then called an implementer) need a license to use those patents.

One of the risks generated by SEPs is that the owners of such patents may unduly block the use of their patented technology by implementers and thus may prevent them from complying with the relevant technical standard. This creates a risk of «patent holdup» to the extent that owners of SEPs can initiate or threaten to initiate patent infringement proceedings in order to obtain potentially excessive royalty payments from implementers and can thus use the threat of injunctive relief as a tactical weapon in order to extract excessive value from their SEPs. Unsurprisingly, this type of behavior has been scrutinized under competition law¹⁰⁴, and measures have been taken to prevent such potentially abusive conduct¹⁰⁵.

Standard-setting organizations (SSOs), as entities which set or develop technical standards, have consequently been requested to take certain measures in order to avoid such potentially abusive behaviors of owners of SEPs. SSOs have specifically been invited to adopt IPR policies under which «participants wishing to have their IPR included in the standard [are requested] to provide an irrevocable commitment in writing to offer to license their essential IPR to all third parties on fair, reasonable and non-discriminatory terms («FRAND commitment»)»¹⁰⁶. This

103 For a general presentation, see (among multiple other publications) the comprehensive Report prepared for the European Commission (Directorate-General for Enterprise and Industry), *Patents and Standards: A modern framework for IPR-based standardization*, 2014 (available at: <http://ec.europa.eu/growth/industry/intellectual-property/patents/standards/index_en.htm>).

104 See the Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements (Text with EEA relevance), OJ C 11, 14.1.2011, p. 1 (available at: <<http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52011XC0114%2804%29&from=EN>>), para. 269; for a (simplified) presentation of the key competition law issues of SEPs, see the Competition policy brief (Issue 8, June 2014) of the European Commission, *Standard-essential patents*, available at: <http://ec.europa.eu/competition/publications/cpb/2014/008_en.pdf> (relating to the Samsung and Motorola cases, whereby this report will focus on the Samsung case).

105 For a recent analysis, see MICHELA ANGELI, *Willing to Define Willingness: The (Almost) Final Word on SEP-Based Injunctions in Light of Samsung and Motorola*, *Journal of European Competition Law & Practice* 2015, p. 221–241.

106 Guidelines (note 104), para. 285; the debate about FRAND licensing has triggered an intensive debate which is reflected in a flurry of scientific publications on these issues, see e.g. CLAUDIA TAPIA, *Industrial Property Rights, Technical Standards and Licensing Practices (FRAND) in the Telecommunications Industry*, Cologne 2010; KNUT BLIND/TIM POHLMANN, *Patente und Standards: Offenlegung, Lizenzen, Patentstreitigkeiten und rechtspolitische Diskussionen*, GRUR 2014, p. 713–719; TIM POHLMANN/KNUT BLIND, *The Interplay of Patents and Standards for ICT*, PIK – Praxis der Informationsverarbeitung und Kommunikation. 2014, Vol. 37, issue 3, p. 189–195; DENNIS W. CARLTON/ALLEN L. SHAMPINE, *Patent Litigation, Standard-Setting Organizations, Antitrust, and FRAND*, 22 *Texas Intellectual Property Law Journal* (2014), p. 223–231; THOMAS F. COTTER, [The] *Comparative Law and Economics of Standard-Essential*

is what was done (by way of illustration) by the European Telecommunications Standards Institute (ETSI) in its IPR Policy¹⁰⁷. The ETSI IPR Policy therefore provides for a mechanism of declaration by which the owners of standard essential patents¹⁰⁸ commit to make their patents available to willing licensees under FRAND terms¹⁰⁹. 6.1 of the ETSI IPR Policy thus provides that:

«[w]hen an ESSENTIAL IPR^[110] relating to a particular STANDARD or TECHNICAL SPECIFICATION is brought to the attention of ETSI, the Director-General of ETSI shall immediately request the owner to give within three months an irrevocable undertaking in writing that it is prepared to grant irrevocable licenses on fair, reasonable and non-discriminatory («FRAND») terms and conditions under such IPR [...]».

Annex A to the ETSI IPR Policy (entitled «IPR Licensing Declaration Forms»)¹¹¹ contains different forms¹¹² to be completed and signed by the owner of the relevant IP rights under which such IP owner is invited to make a formal and binding statement according to which «it and its AFFILIATES are prepared to grant irrevocable licenses under its/their IPR(s) on terms and conditions which are in accordance with Clause 6.1 of the ETSI IPR Policy, [...]»¹¹³.

Patents and FRAND Royalties, 22 Texas Intellectual Property Law Journal (2014), p. 311–363; J. GREGORY SIDA, The meaning of FRAND, part I: royalties, Journal of Competition Law & Economics 2013, p. 931–1055 (available at: <<http://jcle.oxfordjournals.org/content/9/4/931.full>>); J. GREGORY SIDA, The meaning of FRAND, part II: injunctions, Journal of Competition Law & Economics 2015, p. 1–69 (available at: <<http://jcle.oxfordjournals.org/content/early/2015/02/18/joclec.nhv005.full.pdf>>); STEFANO BARAZZA, Licensing standard essential patents, part one: the definition of FRAND commitments and the determination of royalty rates, Journal of Intellectual Property Law & Practice 2014, p. 465–481 (available at: <<http://jiplp.oxfordjournals.org/content/9/6/465.abstract>>); STEFANO BARAZZA, Licensing standard essential patents, part two: the availability of injunctive relief, Journal of Intellectual Property Law & Practice 2014, p. 552–564 (available at: <<http://jiplp.oxfordjournals.org/content/9/7/552.abstract>>); JEREMY MORTON/CHRISTINE GRAHAM, Latest Developments in standards, patents and FRAND licensing, European Intellectual Property Review 2014, p. 700–706.

107 ETSI Intellectual Property Rights Policy (Annex 6 of the Rules of Procedure), available at: <<http://www.etsi.org/images/files/IPR/etsi-ipr-policy.pdf>>; see also the webpage dedicated to IPR: <<http://www.etsi.org/index.php/about/ipr-in-etsi>>.

108 Essential patents are defined as follows in Art. 15.6 of the ETSI IPR Policy (note 107): «ESSENTIAL as applied to IPR means that it is not possible on technical (but not commercial) grounds, taking into account normal technical practice and the state of the art generally available at the time of standardization, to make, sell, lease, otherwise dispose of, repair, use or operate EQUIPMENT or METHODS which comply with a STANDARD without infringing that IPR. For the avoidance of doubt in exceptional cases where a STANDARD can only be implemented by technical solutions, all of which are infringements of IPRs, all such IPRs shall be considered ESSENTIAL».

109 6.1 of the ETSI IPR Policy (note 107).

110 Each of the capitalized terms is defined in article 15 of the ETSI IPR Policy; these terms are not quoted here as they are not of particular relevance for the purpose of the discussion.

111 Available at: <<http://www.etsi.org/images/files/IPR/etsi-ipr-form.doc>> (the «ETSI Declarations»).

112 A «General IPR licensing declaration» and an «IPR information statement and licensing declaration».

113 The relevant fractions of the statements read as follows, for the «General IPR licensing declaration»: «it and its AFFILIATES are prepared to grant irrevocable licenses under its/their IPR(s)

These forms further indicate that their «construction, validity and performance [...] shall be governed by the laws of France»¹¹⁴.

The obviously central element of the debate is the very notion of FRAND licensing¹¹⁵, i.e. what shall be considered fair, reasonable and non-discriminatory licensing terms and conditions, which remains uncertain as of today¹¹⁶ and which shall be discussed below¹¹⁷.

However, a preliminary – and sometimes neglected – legal issue is to analyze carefully the nature and the enforceability of the commitments («undertaking»¹¹⁸) that are made by the owners of the relevant SEPs to the SSOs under the applicable governing law¹¹⁹.

2. *The legal nature of the commitments made by owners of SEPs*

By stating that the owners of SEPs are «prepared to grant irrevocable licenses»¹²⁰ under their SEPs to third party implementers (in their formal undertaking that they make to the SSOs), the issue is whether third party beneficiaries

on terms and conditions which are in accordance with Clause 6.1 of the ETSI IPR Policy, in respect of the STANDARD(S), TECHNICAL SPECIFICATION(S), or the ETSI Project(s), as identified above, to the extent that the IPR(s) are or become, and remain ESSENTIAL to practice that/those STANDARD(S) or TECHNICAL SPECIFICATION(S) or, as applicable, any STANDARD or TECHNICAL SPECIFICATION resulting from proposals or Work Items within the current scope of the above identified ETSI Project(s), for the field of use of practice of such STANDARD or TECHNICAL SPECIFICATION [...]; for the «IPR information statement and licensing declaration»: «To the extent that the IPR(s) disclosed in the attached *IPR Information Statement Annex* are or become, and remain ESSENTIAL in respect of the ETSI Work Item, STANDARD and/or TECHNICAL SPECIFICATION identified in the attached *IPR Information Statement Annex*, the Declarant and/or its AFFILIATES are (1) prepared to grant irrevocable licenses under this/these IPR(s) on terms and conditions which are in accordance with Clause 6.1 of the ETSI IPR Policy [...]».

114 ETSI Licensing Declarations (note 111).

115 From a Swiss perspective, see ROLF H. WEBER, Competition Law versus FRAND Terms in IT Markets, *World Competition Law and Economics Review* 2011, Vol. 34, No. 1, p. 51–71; ROLF H. WEBER/SALIM RIZVI, FRAND – Versuch einer Strukturierung, *RJB/ZBJV* 2011, p. 433–462; FABIO BABEY/SALIM RIZVI, Die Frand-Verpflichtung – Fair, Reasonable and Non-Discriminatory terms (FRAND) im Lichte des Kartellrechts, *WuW* 2012, p. 808–818.

116 See DOUG LICHTMAN, Understanding the RAND Commitment, 47 *Houston Law Review* (2010), p. 1023–1050, p. 1031 available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1783406> («It is something of an outrage that the language of the RAND commitment offers so little guidance as to its proper interpretation.»).

117 See below II.3.

118 Further to the terminology referred to in the ETSI Licensing Declarations (note 111).

119 The goal is not to analyze the relevant issues exclusively or even essentially from the perspective of Swiss law as such (also because Swiss law has not been defined as the governing law in the relevant documents of SSOs which are important for this discussion), but rather to discuss about these legal issues from a more fundamental and policy-oriented perspective (i.e. irrespective of the law that shall apply); the analysis will be made by reference to the ETSI Declarations even if they are to be interpreted under French law, as an example of the types of legal issues that can arise as a result of the commitments made by owners of SEPs.

120 ETSI Declarations (notes 107 and 111).

can request the performance of such obligation, which in turn depends on whether these potential licensees (which have not directly entered into any contract with the owner of the relevant SEPs) can be considered as third party beneficiaries. This issue, which obviously depends on the interpretation of the relevant declaration under the applicable law, remains disputed¹²¹, it being noted that granting – by contract – rights to a third party is generally admitted from a transnational perspective¹²². Under French law, which is of particular relevance for the discussion here (given that it is the law which governs the ETSI Declarations), the view is expressed that the commitments made by owners of SEPs under the ETSI Declarations qualify as «stipulation pour autrui» within the meaning of Art. 1121 of the French Civil Code¹²³.

Interestingly, the Advocate General in the closely watched (on-going) Huawei v ZTE EU case which is pending before the CJEU, drew an analogy between the commitments made by Huawei to ETSI and the «license of right» which is provided for under certain patent regulations¹²⁴. Art. 8 (entitled «Li-

121 Admitting the validity of contractual commitments, see *Microsoft Corp. v. Motorola, Inc.*, 854 F. Supp. 2d 993 (Dist. Court, WD Washington 2012), in which the Court agreed that Motorola's (owner of SEP) through its letters to both the IEEE and ITU [as SSOs], has entered into binding contractual commitments to license its essential patents on RAND terms (with references to prior case law: *Research In Motion Ltd. v. Motorola, Inc.*, 644 F.Supp.2d 788, 797 (N.D. Tex.2008) and *Ericsson Inc. v. Samsung Electronics, Co.*, Civil Action No. 2:06-CV-63, 2007 WL 1202728, at *1 (E.D.Tex. Apr. 20, 2007)) and that Microsoft, as a member of both the IEEE and the ITU, is a third-party beneficiary of Motorola's commitments to the IEEE and ITU (with reference to *ESS Tech., Inc. v. PC-Tel, Inc.*, No. C-99-20292 RMW, 1999 WL 33520483, at *4 (N.D.Cal. Nov. 4, 1999)); these findings were reaffirmed in the subsequent decision *Microsoft Corp. v. Motorola, Inc.*, 864 F. Supp. 2d 1023 (Dist. Court, WD Washington 2012); for an analysis of this case, see KASSANDRA MALDONADO, *Breaching RAND and Reaching for Reasonable: Microsoft v. Motorola and Standard-Essential Patent Litigation*, 29 *Berkeley Tech.L.J.* (2014), p. 419–464, available at: <<http://scholarship.law.berkeley.edu/btlj/vol29/iss4/4>>; for a contractual analysis of FRAND, see ROGER G. BROOKS/DAMIEN GERADIN, *Interpreting and Enforcing the Voluntary FRAND Commitment* (July 20, 2010), available at: <<http://ssrn.com/abstract=1645878>>; for the opposite view (considering that (common law) contract theory does not constitute the proper legal basis for analyzing FRAND), see JORGE L. CONTRERAS, *A Market Reliance Theory for FRAND Commitments and Other Patent Pledges*, to be published in *Utah Law Review* 2015, forthcoming, available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2309023>.

122 See e.g. Art. 5.2.1 (Contracts in favor of third parties) of the 2010 Unidroit Principles of International Commercial Contracts (available at: <<http://www.unidroit.org/instruments/commercial-contracts/unidroit-principles-2010/>>):
«(1) The parties (the «promisor» and the «promisee») may confer by express or implied agreement a right on a third party (the «beneficiary»);
(2) The existence and content of the beneficiary's right against the promisor are determined by the agreement of the parties and are subject to any conditions or other limitations under the agreement».

123 See CHRISTOPHE CARON, *L'efficacité des licences FRAND: entre droit des brevets, droit civil et normalisation*, *La Semaine Juridique*, édition générale, n° 21, 20th May 2013, p. 1006–1013, p. 1008 seq.

124 Opinion of the Advocate General of November 20, 2014 in the case *Huawei Technologies Co. Ltd v ZTE Corp., ZTE Deutschland GmbH* (C-170/13), para. 65: «In this regard, I believe

censes of right») of 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 2012 L 361, p. 1) provides by way of example that «1. The proprietor of a European patent with unitary effect may file a statement with the EPO to the effect that the proprietor is prepared to allow any person to use the invention as a licensee in return for appropriate consideration» (it being noted that the application of this provision will have to be tested once the new system for a European patent with unitary effect shall be fully operational). This «license of right» is also anchored in certain national patent laws¹²⁵. These national provisions – which were adopted long before the FRAND-related disputes in the ICT had emerged – show that stakeholders (including patent owners) can have an interest in declaring in advance their willingness to enter into future patent license agreements. They also show the complexity resulting from a governmental intervention in defining the terms and conditions of the licenses that shall be granted under this legal regime. In this respect, Sec. 46 para. 3 (a) of the UK Patent Act 1977 interestingly provides that, once an entry is made in the register that licenses are available as of right, «any person shall, at any time after the entry is made, be entitled as of right to a license under the patent on such terms as may be settled by agreement or, in default of agreement, by the comptroller on the application of the proprietor of the patent or the person requiring the license». This provision unsurprisingly gives the priority to the freedom of the parties to agree on the terms and conditions of the license, failing which the comptroller shall be requested to define these terms. This power of governmental bodies to define the content of private agreements between contracting parties¹²⁶ is precisely one of the areas

that the commitment given by Huawei in the dispute before the referring court to grant licenses to third parties on FRAND terms bears some similarity to a «license of right». Whereas the grant of compulsory licenses is required by law, a patent owner can on his own initiative authorize third parties to use the teaching of his patent under certain conditions. I would point out that, where a patent licensee has a license of right, an injunction may not, in principle, be issued against him».

125 See Sec. 46 para. 1 of the UK Patent Act 1977 (entitled «Patentee's application for entry in register that licenses are available as of right») which provides that «[a]t any time after the grant of a patent its proprietor may apply to the comptroller for an entry to be made in the register to the effect that licenses under the patent are to be available as of right»; see also § 23 of the German Patent Act (Patentgesetz) para. 1: «Erklärt sich der Patentanmelder oder der im Register (§ 30 Abs. 1) als Patentinhaber Eingetragene dem Patentamt gegenüber schriftlich bereit, jedermann die Benutzung der Erfindung gegen angemessene Vergütung zu gestatten, so ermäßigen sich die für das Patent nach Eingang der Erklärung fällig werdenden Jahresgebühren auf die Hälfte. Die Erklärung ist im Register einzutragen und im Patentblatt zu veröffentlichen».

126 And not only to define the royalty rate to be paid by the licensee to the licensor; in this respect, it is worth noting that the German Patent Act focuses on the issue of the remuneration by establishing a mechanism defining how the remuneration shall be set by the Patent division (see § 23 para. 4 of the German Patent Act). This regulatory focus thus creates the impression that the remuneration would be the only issue to be regulated in the agreement between the licensor and the licensee, which is not the case.

where difficulties may arise, which is illustrated in the on-going debate over the definition of FRAND terms and conditions.

Turning back to FRAND commitments, and by assuming that willing licensees (implementers of the technology standards covered by the SEPs) could be considered as third party beneficiaries of these commitments under the relevant law, the next issue would be to define precisely the legal nature and the scope of the commitments made by the owners of SEPs, i.e. what is the contractual obligation that the owners of SEPs have accepted to perform for the benefit of the potential licensees and that such licensees could directly enforce (as third party beneficiaries)? The specificity and the difficulty of this analysis results from the finding that the relevant obligation does not consist of a straightforward – i.e. easy to identify and thus to enforce – contractual obligation¹²⁷. Quite to the contrary, the owners of SEPs commit to be prepared to license out their patents to third party licensees on FRAND terms and conditions, whereby there remains considerable room as to what shall constitute FRAND terms and conditions¹²⁸.

Under Swiss law (assuming that it would apply), the commitment could be considered as an «agreement to conclude a contract» within the meaning of Art. 22 para. 1 SCO which provides that «[p]arties may reach a binding agreement to enter into a contract at a later date». Pursuant to this provision, one contracting party can promise to its contracting party that it shall enter into a contract with a third party, so that such third party can subsequently request the performance of this obligation (as a third party beneficiary), i.e. it can request that the contract shall be entered into or claim damages for breach of such obligation¹²⁹. The validity of such a preliminary contract (i.e. the contract by

127 By contrast (for the sake of comparison), a contractual obligation which would be simple to enforce by a third party beneficiary would be an obligation of the debtor to pay a given amount to such third party under certain circumstances; for an illustration, see the decision of the Swiss Federal Supreme Court, decision 4C.5/2003 of March 11, 2003 (payment of a financial penalty clause in case of breach of a non-competition undertaking included by two shareholders in a shareholders' agreement, whereby in case of exit by one shareholder and of violation of the non-competition obligation by such shareholder, the payment of the contractual penalty could be enforced directly by the company in which the shareholders held shares: the contractual provision had the following wording: «En cas de départ de la société, interdiction est faite à l'actionnaire sortant de faire concurrence à l'entreprise dans un rayon de 50 km et pendant un délai de 5 ans. Si cette clause devait être violée, une indemnité de 50 000 fr. serait à verser à la société»; this clause was interpreted by the Swiss Federal Supreme Court as granting a direct right to the third party beneficiary (i.e. the relevant company) to request the payment of the contractual penalty from the debtor by application of Art. 112 para. 2 SCO.

128 See e.g. REBECCA HAW ALLENSWORTH, *Casting a FRAND Shadow: The Importance of Legally Defining «Fair and Reasonable» and How Microsoft v. Motorola Missed the Mark*, 22 Texas Intellectual Property Law Journal (2014), p. 235–252.

129 See for instance ATF 98 II 305 para. 1 («Die Architektenklausel zwischen den Parteien des Kaufvertrages ist ein Vorvertrag (Art. 22 OR) zugunsten Dritter, d.h. der Kläger. Diese waren unmittelbar begünstigt und konnten daher nach Art. 112 Abs. 2 OR von der Beklagten verlangen, dass sie den Hauptvertrag abschliesse [...]).

which one party agrees to enter into another future contract) depends on whether the object of the contract is determined or is at least determinable¹³⁰.

From this perspective, the enforceability of the obligation against an owner of SEPs (to execute a license agreement with a third party licensee) will depend on whether such obligation is sufficiently determinable in order to qualify as a valid contractual obligation, the performance of which could be requested and enforced.

In any case, the likely scenario is that an owner of SEP will offer a license on what it considers FRAND terms and conditions to the third party/prospective licensee, which will in turn consider that this offer is not FRAND compliant (particularly because the level of royalties proposed by the owner of SEPs would be too high). The question will thus be whether the potential licensee (as third party beneficiary) could request the enforcement of the obligation of the owner of SEPs. The question will also arise before which court such issue shall be litigated and it is most likely that this issue will be litigated before the court in which the owner of SEPs will have started to enforce its patent against the third party implementer. This consequently means that a court in a given country or more probably several courts located in different countries in which the patent owner will enforce its patents will have to interpret in parallel the same contractual commitments made by the patent owner to the relevant SSO and to define in parallel what could be FRAND terms and conditions, which does not appear as the most efficient mechanism for solving global disputes which originate from one and the same commitment.

In terms of efficiency of the process, it would thus appear appropriate to conceive a mechanism that would reduce the transaction costs which are caused by the negotiation of FRAND terms and conditions, by elaborating guidelines relating to the establishment of FRAND terms and conditions both as to the substance (see immediately below II.3), and as to dispute resolution mechanisms (see below II.4), which could be centralized in order to avoid parallel national court proceedings.

3. *The content of FRAND licenses*

It must be observed from the outset that there is a large variety of legal issues that can arise in FRAND licensing disputes. By way of illustration, it is interesting to note that the ETSI Declarations¹³¹ provide that the owners of SEPs must be «prepared to grant *irrevocable* licenses» (italics added). Leaving aside the interpretation to be given to the concept of irrevocable license under French law, this reference raises the question of the conditions under which a FRAND compliant license can be terminated, which in turn refers to the law which shall

¹³⁰ ATF 118 II 32 para. 3b; ATF 98 II 305 para. 1.

¹³¹ Note 111.

govern the license (it being noted that the ETSI Declarations do not prescribe that the license agreements to be entered on FRAND terms and conditions shall be governed by French law)¹³². From the standpoint of Swiss contract law (assuming that the license agreement would be governed by Swiss law)¹³³, it would not be possible for the owner of SEPs to grant irrevocable licenses, foremost because a party to a long term contract governed by Swiss law has the unwaivable right to terminate the agreement for just cause pursuant to a general principle anchored under Swiss contract law¹³⁴. On this basis, depending on the governing law, a license agreement on SEPs could or could not be irrevocable. Several other issues could also arise including the contractual conditions under which the license could be terminated: does the obligation of the licensor to comply with FRAND, and specifically the conditions of fairness and of reasonableness, mean that the agreement cannot give to the licensor (and owner of SEPs) the right to terminate the license in case of late payment of royalty fees by the licensee? If an early termination of the license is possible in case of breach (which would appear quite reasonable), what shall be the cure period in case of late payment before the license can be terminated (30 days?)? What shall be the liability of the licensor in case of invalidity of (one of) the licensed patent(s): shall the licensor reimburse the royalty fees that it would have collected until the time of cancellation of the relevant patent from the patent registry because this would potentially be required in order to be FRAND compliant?

This raises the issue of the (contractual) scope of FRAND terms and conditions. While the FRAND debate has largely focused on the assessment and calculation of FRAND compliant royalties¹³⁵, patent licensing agreements contain a range of other terms and conditions for which the question of their compliance with FRAND terms may also arise¹³⁶.

132 Whereby it is clear that in most cases the license agreement will be entered between companies which will be located in different countries so this will be an international agreement for which the issue of the governing law will arise.

133 Which is relatively frequently chosen as governing law in international technology related agreements, as resulting from a recent survey, see the Results of the WIPO Arbitration and Mediation Center International Survey on Dispute Resolution in Technology Transactions (March 2013), available at: <<http://www.wipo.int/export/sites/www/amc/en/docs/surveyresults.pdf>>, p. 15.

134 MARIE-NOËLLE VENTURI ZEN-RUFFINEN, La résiliation pour justes motifs des contrats de durée, Fribourg 2007, p. 115 N. 330 seq.

135 See GUNTHER FRIEDL/CHRISTOPH ANN, Entgeltberechnung für FRAND-Lizenzen an standard-essenziellen Patenten, GRUR 2014, p. 948–955.

136 See JORGE L. CONTRERAS/DAVID L. NEWMAN, Developing a Framework for Arbitrating Standards-Essential Patent Disputes, Journal of Dispute Resolution 2014, p. 23–51, p. 39, referring to «Non-Royalty FRAND Terms» available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2335732>; see also JAMES H. CARTER, FRAND Royalty Disputes: A New Challenge for International Arbitration?, in: Arthur W. Rovine (ed.), Contemporary Issues in International Arbitration and Mediation – the Fordham Papers 2013, Leiden/Boston 2013, p. 67–78, p. 73 (holding that «[t]he paradigm license term in dispute naturally would be a royalty rate or rates,

It results from these observations that it would appear adequate to establish common global guidelines and policies for the purpose of defining the *mechanisms* by which FRAND terms shall be defined as well as the *substantive* meaning and interpretation of such terms on the basis of harmonized transnational legal principles.

The complexity of these issues is further increased by the mobility of patent portfolios which are and remain tradable (intangible) assets. It is thus frequent that SEPs are transferred by their owners to third parties. The question consequently is: do the commitments made by the owners of SEPs to the SSOs go along to the new owners of the SEPs? Ideally, this should be addressed in the contract by which the SEPs are assigned by inserting provisions to that effect. If there is no contractual solution, an analysis has to be conducted under local intellectual property laws in order to assess whether encumbrances relating to patents which have been accepted by the former patent owner are transferred to the new patent owner. Under Swiss patent law (assuming that a Swiss patent would be part of a portfolio of SEPs that would have been transferred to a third party), Art. 34 para. SPA provides that «[l]icences of third parties not recorded in the Patent Register are invalid against persons who have acquired in good faith the rights to the patent». The difficulty is however that this provision does not directly apply to the situation at issue because the commitments made by owners of SEPs to SSOs (as resulting from the ETSI Declarations) are not licenses granted by the patent owner to a third party. These commitments may indeed only subsequently lead to the conclusion of one or several license agreements. It is therefore uncertain that such commitments could be opposed to third parties under Swiss law even if they were recordable and recorded in the Swiss patent registry. Similar difficulties are likely to arise under many national patent laws, in spite of the largely shared perception that these commitments should pass to the new owner¹³⁷. In view of this situation, measures have been taken in order to maximize the chances that these commitments shall follow the transfer of the SEPs and shall also be binding on their new owner¹³⁸.

on the setting of which large amounts of money could turn; but there might be dozens of other disputed terms, many with complicated (but not readily apparent) financial implications. Patent license agreements can be complex documents»); see also WEBER, *Competition Law vs FRAND Terms in IT Markets* (note 115), p. 56 (who considers that «‘fair’ relates to the underlying licensing terms, [and] ‘reasonable’ refers to the licensing rates»).

137 See ITU Report (note 101), p. 70: «Strong consensus has developed in various SDOs, however, that patent obligations should ‘run with the patent’ when patent rights are assigned, and that RAND commitments should be construed as encumbrances that bind all successors-in-interest to the RAND declarant. However, SDO participants recognize that this interpretation may not apply in all jurisdictions»; see also JAY P. KESAN/CAROL M. HAYES, *FRAND’s Forever: Standards, Patent Transfers, and Licensing Commitments*, 89 *Indiana Law Journal* (2014), p. 231–314, available at: <<http://ssrn.com/abstract=2226533>>.

138 This is what was done in the ETSI IPR Policy (note 107): 6.1bis Transfer of ownership of ESSENTIAL IPR «FRAND licensing undertakings made pursuant to Clause 6 shall be interpreted as encumbrances that bind all successors-in-interest. Recognizing that this interpretation may

4. *FRAND dispute resolution mechanisms*

Given that the commitments made by the owners of SEPs do not solve all potential disputes between them and potential third party licensees and that owners of SEPs may be inclined to use patent remedies (and request injunctive relief against potential licensees/implementers), the adoption of balanced and efficient dispute resolution mechanisms is essential in order to preserve the legitimate interests of all stakeholders, and particularly those of the implementers which may be unduly affected by injunctions of owners of SEPs.

This can be illustrated by the high profile Samsung v Apple dispute which led to an EU antitrust procedure¹³⁹ that was closed on April 29, 2014 by a decision of the EU Commission¹⁴⁰.

By this decision, the Commission accepted the legally binding commitments made by Samsung (hereinafter: «the Commitments»)¹⁴¹, which are of high importance because they illustrate the type of processes that have been validated in order to solve FRAND-related disputes¹⁴².

The relevant elements of the case are as follows: Samsung owns SEPs related to the 3G UMTS¹⁴³ standard (which is an industry standard for mobile and wireless communications). Samsung committed to license its SEPs on FRAND terms and conditions pursuant to the relevant ETSI rules. Samsung started to enforce certain of its UMTS SEPs against Apple in various EU countries (France, Germany, Italy, the Netherlands and the United Kingdom) in which it sought to obtain preliminary and permanent injunctions from the courts. The EU Commission initiated antitrust proceedings in order to investigate whether Samsung had failed to honor the commitment it gave to ETSI

not apply in all legal jurisdictions, any Declarant who has submitted a FRAND undertaking according to the POLICY who transfers ownership of ESSENTIAL IPR that is subject to such undertaking shall include appropriate provisions in the relevant transfer documents to ensure that the undertaking is binding on the transferee and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding all successors-in-interest. The undertaking shall be interpreted as binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents».

139 Case AT.39939 – Samsung – Enforcement of UMTS standard essential patents; see <http://ec.europa.eu/competition/elojade/iseff/case_details.cfm?proc_code=1_39939>.

140 Commission Decision of 29 April 2014 relating to a proceeding under Article 102 of the Treaty on the functioning of the European Union and Article 54 of the EEA Agreement (Case AT.39939 – Samsung – Enforcement of UMTS standard essential patents) (notified under document number C(2014) 2891 final), available at: <http://ec.europa.eu/competition/antitrust/cases/dec_docs/39939/39939_1501_5.pdf> (the summary of the decision was published in OJ 2014/C 350/08 of October 4, 2014).

141 The Commitments are available at: <http://ec.europa.eu/competition/antitrust/cases/dec_docs/39939/39939_1502_5.pdf>.

142 This section of the report is derived from JACQUES DE WERRA, The expanding significance of arbitration for patent licensing disputes: From post-termination disputes to pre-licensing FRAND disputes, ASA Bulletin 2014, vol. 32, no. 4, p. 692–706, available at: <<http://archive-ouverte.unige.ch/unige:46142>>.

143 Universal Mobile Telecommunications System.

that it would license its SEPs on FRAND terms (i.e. whether Samsung has failed to honor its FRAND commitment in licensing negotiations, including by seeking injunctive relief before the courts of certain Member States in relation to some of its SEPs). In the course of its investigation, the Commission preliminarily concluded that Samsung's seeking of preliminary and permanent injunctions against Apple on the basis of its SEPs, in view of the exceptional circumstances of the case and in the absence of any objective justification, raised concerns as to the compatibility of the seeking of such injunctions with Art. 102 of the Treaty on the functioning of the European Union (TFEU). The exceptional circumstances were the UMTS standard-setting process and Samsung's commitment to license its SEPs on FRAND terms and conditions. The absence of objective justification related in particular to the fact that the potential licensee, i.e. Apple, was not unwilling to enter into a license agreement for Samsung's SEPs on FRAND terms and conditions.

By its decision of April 29, 2014, the Commission validated the Commitments made by Samsung¹⁴⁴ and decided that they shall be binding on Samsung (and Samsung's affiliates) for a period of five years and consequently concluded that there were no longer grounds for action by the Commission.

The Commitments are extremely interesting from a dispute resolution perspective, given that they provide for the submission to court proceedings or arbitration of FRAND disputes as part of a sophisticated and multi-step negotiation and dispute resolution mechanism. The Commitments first provide for the creation of a so-called «Licensing Framework» the objective of which is to determine FRAND licensing terms between Samsung and potential licensees¹⁴⁵. The Licensing Framework institutes a mandatory negotiation period (in principle 12 months) during which Samsung and the potential licensee are invited to negotiate on FRAND terms with a view to agreeing on a unilateral license or a cross-license. If the negotiations fail and if the parties do not agree on an alternative procedure for determining FRAND terms, the Commitments provide that «the Parties shall submit the matter to arbitration or to court adjudication in order to determine the FRAND terms of a Unilateral License or, as applicable a Cross-License [...]»¹⁴⁶ in the course of a phase called «Third Party Determination of FRAND Terms»¹⁴⁷. The Parties are then invited to jointly decide whether they shall submit the FRAND dispute to arbitration or court adjudication within a given time limit, whereby in the absence of agreement, the dispute will be submitted to courts¹⁴⁸.

¹⁴⁴ See note 140.

¹⁴⁵ The Commitments (note 141) provide for the opportunities to negotiate cross-licenses (in the case Samsung's licensees are also owners of SEPs).

¹⁴⁶ Commitments (note 141), clause 1.b.

¹⁴⁷ Commitments (note 141), clause 1.b.

¹⁴⁸ Pursuant to the Commitments (note 141), clause 10: «[t]he venue for the court adjudication procedure will be the Patent Court, High Court of England and Wales (or any successor court), or

The Commitments provide for quite detailed rules on the arbitration proceedings. They first opt for institutional arbitration by indicating that «the dispute shall be finally settled under the rules of arbitration of the ICC, unless the Parties mutually agree that the arbitration tribunal will be the patent mediation and arbitration centre as established under Art. 35(1) of the Agreement on a Unified Patent Court»¹⁴⁹. The reference to the patent mediation and arbitration center to be established under the UPC (Art. 35) is quite interesting because of the specificities of the center¹⁵⁰. It confirms the potential importance that this center could gain as provider of arbitration and mediation services for intellectual property (and specifically patent) disputes in the future¹⁵¹. The arbitration procedure envisioned in the Commitments has several notable features. The Commitments first provide that «[a] non-confidential version of the arbitral decision shall be published within 90 days following the issuance of such decision» and that «[t]he non-confidential version of the arbitral decision may disclose the methodology relied upon by the arbitral panel to arrive at specific FRAND terms, but shall in no event disclose specific terms»¹⁵². This unusual element, which stands in obvious conflict with the basic tenet of confidentiality in commercial arbitration, is due to the requirement of transparency of FRAND decisions and awards reflected in the decision of the Commission of April 29, 2014¹⁵³.

The justification of the public disclosure of FRAND-related arbitral awards is debated in the legal literature¹⁵⁴. One issue to consider is the value and usefulness of the information contained in an arbitral award that shall potentially be disclosed to the public. In this respect, we may wonder if the publication of only the FRAND

the UPC» [i.e. the Unified Patent Court as instituted by the Agreement on a Unified Patent Court of February 19, 2013, available at: <<http://www.upc.documents.eu.com/>>].

149 Commitments (note 141), clause 9.a.

150 It is noteworthy that the center shall have two seats in Ljubljana and Lisbon (Art. 35 para. 1 UPC).

151 The center has not been established yet and has not published its arbitration and mediation rules (that shall be adopted by the Center pursuant to Art. 35 para. 3 UPC); for an analysis, see JACQUES DE WERRA, *New Developments of IP Arbitration and Mediation in Europe: The Patent Mediation and Arbitration Center Instituted by the Agreement on a Unified Patent Court*, *Revista Brasileira de Arbitragem* 2014, p. 17–35 (available at: <<http://archive-ouverte.unige.ch/unige:39878>>); it also remains to be seen whether the Center will adopt specific procedures and principles for FRAND disputes.

152 Commitments (note 141), clause 9.e.

153 Decision of the Commission (note 140), para. 111 («the publication of a non-confidential version of arbitration awards will contribute to the creation of a body of case-law upon which future FRAND determinations could draw. This should contribute to a principled and efficient solution of future FRAND disputes by arbitration tribunals»).

154 See YOONHEE KIM, *Lifting Confidentiality of FRAND Royalties in SEP Arbitration*, 16 *Columbia Science & Technology Law Review* (2014), p. 1–35, available at: <<http://stlr.org/volumes/volume-xvi-2014-2015/lifting-confidentiality-of-frand-royalties-in-sep-arbitration/>>; for an opposing view (preserving the confidentiality of arbitration), see DAMIEN GERADIN, *Confidentiality of FRAND Royalties in Arbitration*, available at: <<https://frandlitigationarbitration.wordpress.com/2015/02/28/confidentiality-of-frand-royalties-in-arbitration/>>.

licensing rate would be relevant¹⁵⁵, knowing that the royalty rate will likely also reflect the validity of the licensed SEPs at issue, the relative value of the asserted patents both to the technical standard and to the infringing product¹⁵⁶. On this basis, it is uncertain whether the disclosure of the sole royalty rate could be of significant value. Another aspect relates to the non-discriminatory element of FRAND licensing. This requirement of non-discrimination presupposes that decision-makers (and specifically arbitral tribunals) shall have access to other decisions and licenses in order to ensure that this condition of non-discrimination is met¹⁵⁷. It however remains that non-discrimination does not necessarily imply that all the licensing terms and conditions and all the license agreements shall be identical¹⁵⁸. It would be worth considering the adoption of certain guidelines about the publication of FRAND-related arbitral awards (whereby certain confidential sections could be redacted in order to find an equitable balance between confidentiality and transparency¹⁵⁹) and to entrust a third party (potentially an arbitration institution) with the mission of communicating the relevant information to the arbitral tribunals, or even with the mission to review and scrutinize draft arbitral awards in order to ensure a certain consistency between the awards that shall be rendered under its supervision on FRAND licensing disputes.

The Commitments further provide for a «de novo appeal on issues of fact and law» against an arbitral award¹⁶⁰ before another arbitral tribunal¹⁶¹, whereby the «appeal shall be treated as a separate arbitration»¹⁶² in which the parties can «agree to limit the issues to be considered on appeal»¹⁶³. This constitutes another unusual feature of these proceedings which stands in sharp contrast to standard commercial arbitration practice. Interestingly, the Commitments state in this respect with regard to the seat of the arbitration that it «will be in an EEA jurisdiction in which national laws permit Parties to agree to make an arbitration decision subject to appeal to a second arbitral tribunal»¹⁶⁴.

155 This is what is pleaded for by KIM (note 154), p. 32, who concludes his article by stating that «[t]his Article does not argue that all patent licensing terms be known to the public: only a FRAND licensing rate calls for scrutiny in light of its public nature».

156 See CONTRERAS/NEWMAN (note 136), p. 37.

157 CARTER (note 136), p. 78.

158 See WEBER (note 115), p. 56 (noting that the non-discrimination obligation «does not exclude that licensing terms are dependent on the volume of the ordered goods or the creditworthiness of the licensee»).

159 See CARTER (note 136), p. 78.

160 «the first arbitral tribunal's decision» (according to the terminology of the Commitments (note 141), clause 9.f.).

161 «the second arbitral tribunal» (according to the terminology of the Commitments (note 141), clause 9.f.i), whereby reference is also made to «the second arbitral panel», Commitments (note 141), clause 9.f.ii).

162 Commitments (note 141), clause 9.f.v.

163 Commitments (note 141), clause 9.f.iii.

164 Commitments (note 141), clause 9.d; the Commitments remain silent as to whether and under what conditions an appeal can be lodged against the award rendered on appeal by «the second

Thirdly, the Commitments indicate, as to the substantive scope of the jurisdictional power of the arbitral tribunal that «[t]he arbitral panel shall take into account issues of validity, infringement, essentiality raised by the Parties in making the Third-Party Determination of FRAND Terms»¹⁶⁵. This is interesting because it shows that arbitral tribunals¹⁶⁶ may have to take into account potential claims of invalidity of the disputed SEPs. This is of particular relevance to the extent that this confirms that it is legitimate that arbitral tribunals shall have the power to «take into account» these issues¹⁶⁷.

Another issue is to define under which (patent) law(s) the issues of (in)validity and (non-) infringements of SEPs will have to be decided in view of the clause of the Commitments providing that «[t]he arbitration will be governed by the laws of England and Wales»¹⁶⁸. The question arises whether this provision was meant and was supposed to constitute a choice of law clause which could potentially mean that all issues that may arise in the arbitration (including issues of validity or infringement of the SEPs) should be decided under the laws of England and Wales. This would be possible in view of the freedom of the parties to select the governing law in international commercial arbitration. This flexibility and liberalism of arbitration stand in sharp contrast to the rigidity of choice of law rules which apply before national courts¹⁶⁹.

The Samsung case shows in any event that arbitration is viewed as a sustainable alternative to court litigation for solving FRAND disputes¹⁷⁰ and has been

arbitral tribunal» which will ultimately depend on the law applicable in the jurisdiction of the seat of the arbitration.

165 Commitments (note 141), clause 9.g.

166 It appears that this rule (in view of its systematic position in the Commitments) shall apply to both the «first arbitral tribunal» and to the «second arbitral tribunal».

167 The Commitments do not address the potential effects of an award rendered by the arbitral tribunal finding a SEP invalid. It should however be assumed that this will be limited to the parties, i.e. *inter partes* (and not *erga omnes*), also because of the wording of the Commitments which indicate that the arbitral tribunal shall «take into account» these issues, and which does not indicate that the arbitral tribunals shall have the power to decide as such on the invalidity of a given SEP. For arbitration disputes submitted to the patent mediation and arbitration center under the UPC, Art. 35 para. 2 *in fine* UPC expressly provides that «a patent may not be revoked or limited in mediation or arbitration proceedings» so that arbitral tribunals would not have the power to revoke a patent in that case.

168 It is uncertain whether the goal of this provision was to address the law applicable to the relevant patent issues (particularly their infringement and their validity).

169 Art. 8 of the Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II) indeed provides that «[t]he law applicable to a non-contractual obligation arising from an infringement of an intellectual property right shall be the law of the country for which protection is claimed» (Art. 8 para. 1), whereby this choice of law rule is mandatory and thus cannot be derogated from by contract (Art. 8 para. 3); on this issue (and on potential advantages of arbitration), see JACQUES DE WERRA, Arbitrating International Intellectual Property Disputes: Time to Think Beyond the Issue of (Non-) Arbitrability, *International Business Law Journal* 2012, Issue 3, p. 299–317, p. 307 seq. (available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2149762>).

170 This is also confirmed by other antitrust proceedings relating to FRAND licensing, and particularly by the US case *In re Motorola Mobility LLC, and Google Inc.*, available at: <<http://www>

validated as such by competition authorities. It is therefore not surprising that efforts have been made by major institutions in order to address the needs of companies involved in FRAND licensing disputes and to conceptualize new dispute resolution mechanisms that shall be tailored to such disputes¹⁷¹. The WIPO Arbitration and Mediation Center has consequently established specific submission agreements that are adapted to FRAND Disputes¹⁷² and the International Telecommunication Union (ITU) continues to be active on these issues¹⁷³.

The implementation of FRAND commitments still raises major difficulties today and consequently continues to be discussed in the relevant fora¹⁷⁴. The European Commission has also launched (which ran from October 14, 2014 to February 15, 2015) a public consultation on patents and standards in order to gather information and views on the interplay between standardization and intellectual property rights (IPR), and particularly patents¹⁷⁵. The questionnaire which was submitted in the course of this public consultation contained a list of detailed questions relating to the «benefits and costs of dispute resolution mechanisms»¹⁷⁶ and particularly discussed the advantages and disadvantages

ftc.gov/enforcement/cases-proceedings/1210120/motorola-mobility-llc-google-inc-matter>; in its decision and order of July 23, 2013 (available at: <<http://www.ftc.gov/sites/default/files/documents/cases/2013/07/130724googlemotorolado.pdf>>), the Federal Trade Commission validated arbitration as a means «to establish a License Agreement» (para. I.D) under SEPs owned by Motorola to willing licensees; arbitration is also selected by other technical bodies in order to solve FRAND-related SEPs licensing disputes; this is the case of the DVB (Digital Video Broadcasting) Project (<<http://www.dvb.org>>); Art. 14.7 of its Statutes (also referred to as «Memorandum of Understanding», available at: <http://www.dvb.org/resources/public/documents_site/dvb_mou.pdf>) provides for the submission to arbitration of disputes arising between Members about IPR licensing as follows: «Each Member hereby agrees, on its behalf and on behalf of its affiliated companies, that, subject to clause 14.9 of this Article 14, all disputes with any other Member of these statutes (MoU) regarding solely the terms and conditions of licenses arising in connection with the undertaking in this Article 14 shall be finally settled under the Rules of Conciliation and Arbitration of the International Chamber of Commerce by three arbitrators appointed in accordance with such Rules. Arbitration shall take place in Frankfurt, Germany».

171 See CONTRERAS/NEWMAN (note 136), p. 46, indicating that they chair a group instituted under the aegis of the American Bar Association that is seeking to develop best practices for the arbitration of SEP disputes (called the «ABA SEP Arbitration Project (ASAP)»).

172 See the specific submission agreements that are tailored to FRAND Disputes <<http://www.wipo.int/amc/en/center/specific-sectors/ict/frand/>>; for a presentation, see HEIKE WOLLGAST/IGNACIO DE CASTRO, WIPO Arbitration and Mediation Center: New 2014 WIPO Rules; WIPO FRAND Arbitration, ASA Bull. 2/2014, p. 286–296, at p. 290 seq.

173 See the excellent report of the ITU (note 101), Understanding patents, competition and standardization in an interconnected world (July 1, 2014), available at <<http://www.itu.int/en/ITU-T/Workshops-and-Seminars/patent/Pages/default.aspx>>; see also the site of the «ITU Patent Roundtable», available at: <<http://www.itu.int/en/ITU-T/Workshops-and-Seminars/patent/Pages/default.aspx>>.

174 See in particular the work of the ETSI IPR Committee (note 107); this is also reflected in the legal literature, see the references cited in note 106.

175 See <<http://ec.europa.eu/DocsRoom/documents/7163/attachments/1/translations/en/renditions/native>> (from which the questionnaire can be downloaded).

176 See questions Q7.2.1 to 7.2.5 of the survey (note 175).

of arbitration (and ADR) for solving FRAND disputes. It will be important to monitor the next steps of this process. On the judiciary front, the CJEU is expected to render a major decision in the case *Huawei Technologies Co. Ltd v ZTE Corp., ZTE Deutschland GmbH* (C-170/13) which should clarify the obligations of owners of SEPs under competition law, particularly regarding the conditions under which injunctive relief can be obtained by them and in the affirmative under what conditions¹⁷⁷.

It is in any case important to ensure that fair and equitable dispute resolution mechanisms shall be adopted to solve FRAND patent licensing disputes, whereby arbitration could play a significant role in this context, as evidenced by certain proposals which have suggested arbitration as the exclusive dispute resolution mechanism for solving FRAND disputes in certain circumstances¹⁷⁸.

5. Conclusion

The debate about FRAND licensing shows that the transaction costs resulting from licensing negotiations can be very high¹⁷⁹, which calls for a certain work of *legal standardization*.

In order to be efficient, FRAND terms and conditions should be standardized. The process of *technical standardization* which has led to the development of the concept of FRAND licensing terms and conditions should consequently lead to a *legal standardization* of these terms and conditions

177 The first of the questions submitted to the CJEU by the referring court (the Landgericht Düsseldorf) in its request for a preliminary ruling lodged on April 5, 2013 is: «Does the proprietor of a standard-essential patent who informs a standardisation body that he is willing to grant any third party a licence on fair, reasonable and non-discriminatory terms abuse his dominant market position if he brings an action for an injunction against a patent infringer although the infringer has declared that he is willing to negotiate concerning such a licence?»; the opinion of the Advocate General (Melchior Wathelet) was delivered on November 20, 2014; from a dispute resolution/arbitration perspective, the opinion quite interestingly indicates (§ 40) that «[t]he questions raised by the referring court do not concern the specific terms of a FRAND licence, which lie in the discretion of the parties and, where appropriate, the civil courts and arbitration tribunals», thereby confirming that arbitral tribunals shall also have the power to decide on these issues; it remains to be seen whether and, in the affirmative, to what extent, the Court will follow the opinion of the Advocate General.

178 See MARK A. LEMLEY/CARL SHAPIRO, A Simple Approach to Setting Reasonable Royalties for Standard-Essential Patents, 28 Berkeley Technology Law Journal (Fall 2013), p. 1135–1166 (available at: <http://btlj.org/data/articles/2015/vol28/28_2/28-berkeley-tech-l-j-1135-1166.pdf>), who have proposed that the standard-essential patent owner shall be obligated to enter into binding baseball-style (or «final offer») arbitration with any willing licensee to determine the royalty rate; for a critical analysis of their proposal, see PIERRE LAROUCHE/JORGE PADILLA/RICHARD S. TAFFET, Settling FRAND Disputes Is Mandatory Arbitration a Reasonable and Non-Discriminatory Alternative?, Journal of Competition Law & Economics 2014, p. 581–610 (available at: <<http://jcle.oxfordjournals.org/content/10/3/581.abstract>>).

179 See the interesting paper (under copyright law) of PETER S. MENELL/BEN DEPOORTER, Using Fee Shifting: A Proposal to Promote Fair Use and Fair Licensing, 105 California Law Review (2014), p. 53–86, available at: <<http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=3270&context=facpubs>>.

(*substantive* legal standards) and to the standardization of the processes and mechanisms (*procedural* legal standards) which can lead to their use in a specific case, i.e. to the negotiation and conclusion of a FRAND compliant license agreement.

FRAND licensing thus shows the complexities of harmonization of patent licensing transactions as to the substance (i.e. what shall be held as fair, reasonable and non-discriminatory licensing terms and conditions) and as to the processes (i.e. how shall FRAND licensing disputes be efficiently solved). Even if FRAND licensing terms and FRAND-related legal issues clearly have specific features which cannot necessarily be found in other areas of intellectual property licensing, the discussion about FRAND licensing cannot avoid the finding that the law of intellectual property licensing is more generally still underdeveloped at the international and even regional level and that this situation is inadequate¹⁸⁰. The opportunity offered by the debate surrounding FRAND licensing should consequently be seized in order to conceptualize transnational licensing principles.

The discussion about FRAND licensing reveals in any event the lack of a deeper understanding of what shall constitute fair and reasonable licensing terms and conditions from a transnational perspective. It may appear surprising that the law governing intellectual property licensing transactions remains largely unaffected by global trends of harmonization in spite of the unanimous understanding that intellectual property transactions as such, and licensing agreements in particular, are essential in today's interconnected world and economy. On this basis, FRAND licensing shows the interest and even the need to develop common global standards of fair and reasonable licensing terms. This need is further confirmed by the development of compulsory licensing mechanisms which raise similar issues, i.e. what shall be the standard terms and conditions of a compulsory license¹⁸¹? In the absence of source of global guidance¹⁸²,

180 For a presentation of various perspectives of licensing practices in various countries and from various policy standpoints, see JACQUES DE WERRA (ed.), *Research Handbook on Intellectual Property Licensing*, Cheltenham (UK)/Northampton (USA) 2013 (<<http://www.ip-licensing.info>>).

181 It is worth mentioning that compulsory licensing mechanisms are also attracting increased scientific attention, see the collective book: RETO M. HILTY/KUNG-CHUNG LIU (eds), *Compulsory Licensing: Practical Experiences and Ways Forward*, MPI Studies in Intellectual Property and Competition Law No 22, Munich 2015.

182 Art. 31 TRIPS does not define the detailed conditions under which compulsory licenses shall be granted and many issues are still open; for instance, how can the patent owner and licensor control whether the compulsory licensee pays the adequate level of royalties (i.e. can there be an audit?)? Is there an implied warranty of validity or title of the patent owner? Can the compulsory license be terminated beyond the scenario identified in Art. 31 para. g TRIPS (which provides that «authorization for such use shall be liable, subject to adequate protection of the legitimate interests of the persons so authorized, to be terminated if and when the circumstances which led to it cease to exist and are unlikely to recur. [...]»), for instance because of a material breach committed by the licensee, etc.

local courts will establish their own standards which may lead to conflicting solutions from a transnational perspective¹⁸³.

The FRAND licensing debate also raises the difficult question of the role of competition law in solving these issues at the crossroads of diverse legal fields, including contract law and intellectual property law (and also to the interactions between these two fields)¹⁸⁴. While it is clear and undisputable that competition law is of key importance in this debate and that it must consequently not be underestimated, it still seems doubtful to admit that mechanisms which have been validated by competition authorities (such as the Commitments of Samsung commented above) shall be viewed as the ultimate standards of reference for all purposes, and specifically from a dispute resolution perspective¹⁸⁵. As discussed above, the Commitments raise complex issues which will need to be duly reflected upon in order to establish adequate and ideally global substantive and procedural standards for solving FRAND disputes.

C. Trade Secrets

I. Introduction

In an era where access to and control of information are of key importance and in which cyber security risks seriously threaten corporate trade secrets¹⁸⁶, it is

183 See, by way of example, the dispute about the grant of a compulsory license between Bayer and Natco in India as resulting from the Decision of the Intellectual Property Appellate Board («IPAB») of Chennai of March 4, 2013 (OA/35/2012/PT/MUM); decision of the Controller of Patents Mumbai of March 9, 2012; appeals against the decision of the IPAB were dismissed by the Bombay High Court (see: <<http://spicyip.com/2014/07/spicyip-tidbit-bombay-hc-dismisses-challenge-to-nexavar-compulsory-license.html>>) and by the Indian Supreme Court (which dismissed Bayer's Special Leave Petition, see: <<http://court.nic.in/supremecourt/temp/sc%203014514p.txt>>).

184 For quite a vehement position criticizing the interference of competition law in the intellectual property system, see ROBIN JACOB, Competition Authorities Support Grasshoppers: Competition Law as a Threat to Innovation, Competition Policy International, Vol. 9, Number 2, Autumn 2013, p. 15–29 (concluding his paper (p. 26) by stating that «[t]he Competition Authorities should cease harassing inventive industries, remember that patents expire anyway and let the patent system do the job it was designed to do. Leave the ants alone»).

185 See CARTER (note 136), p. 72 seq. (scrutinizing the FTC's proposed and final consent orders in the US Motorola – Google dispute from an arbitration standpoint, whereby these comments can apply to other competition law proceedings in FRAND disputes).

186 See DAVID S. ALMELING, Seven Reasons Why Trade Secrets Are Increasingly Important, 27 Berkeley Technology Law Journal (2012), p. 1091–1118 (listing digital technology as the first of the seven reasons of the growing importance of trade secrets), and stating that (p. 1094) «[t]he revolution in digital storage – cloud computing, e-mail, thumb drives – makes it easier to take trade secrets, whether the culprit is an employee who copies company secrets on a thumb drive or a hacker who breaches the company's network from thousands of miles away», available at: <<http://scholarship.law.berkeley.edu/btlj/vol27/iss2/4/>>; see by way of illustration the case *United States v. Genovese*, 409 F. Supp. 2d 253, 255 (S.D.N.Y. 2005) (in which the defendant was charged with selling Microsoft source code on the Internet); see also JOHN VILLASE-

essential to assess how confidential information can be legally protected against its misappropriation by unauthorized third parties¹⁸⁷.

In view of these new threats, it is not surprising that the protection of trade secrets (which constitutes «undisclosed information»¹⁸⁸) has come to the forefront of the political agenda in many parts of the world, including in the United States of America, which has launched a strategy for «mitigating the theft of U.S. trade secrets»¹⁸⁹ and which has also improved its regulatory framework¹⁹⁰. On July 29, 2014, North Carolina Congressman George Holding introduced the Trade Secrets Protection Act of 2014, H.R. 5233¹⁹¹, which seeks to create a private federal remedy for victims of trade secret theft in the face of growing cyber threats¹⁹².

This is also the case in the European Union which launched a consultation for the purpose of assessing the need to strengthen the legal protection of trade secrets¹⁹³ and is presently in the process of adopting a Directive on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure¹⁹⁴.

NOR, Corporate Cybersecurity Realism: Managing Trade Secrets in a World Where Breaches Occur (to be published in the American Intellectual Property Law Association Quarterly Journal, 2015), available at: <<http://hooverip2.org/wp-content/uploads/ip2-wp14012-paper.pdf>>; MARCO ALEXANDRE SAIAS, Unlawful acquisition of trade secrets by cyber theft: between the Proposed Directive on Trade Secrets and the Directive on Cyber Attacks, Journal of Intellectual Property Law & Practice 2014, vol. 9, p. 721–729; see already BRUCE T. ADKINS, Note, Trading Secrets in the Information Age: Can Trade Secret Law Survive the Internet?, University of Illinois Law Review (1996), p. 1151–1196.

187 This paper will not address the topic of data privacy and data surveillance, even if it is obviously also of high importance for private individuals and for companies in today's interconnected world, as evidenced by the scandal about the U.S. National Security Agency data online surveillance program (Prism program).

188 Pursuant to the terminology of Art. 39 TRIPS, see below C.II.

189 See the paper released on February 20, 2013, «Administration Strategy on Mitigating the Theft of U.S. Trade Secrets», available at: <<http://www.whitehouse.gov/blog/2013/02/20/launch-administration-s-strategy-mitigate-theft-us-trade-secrets>>.

190 I.e. the Theft of Trade Secrets Clarification Act of 2012 (available at: <<http://thehill.com/images/stories/blogs/flooraction/jan2012/s3642.pdf>>) and the Foreign and Economic Espionage Penalty Enhancement Act of 2012.

191 Available at: <http://holding.house.gov/sites/holding.house.gov/files/documents/TSPA%20-%20HOLDNC_018_xml.pdf>.

192 See the statement made by Congressman GEORGE HOLDING «American businesses face relentless cyber security threats every day, costing our economy billions of dollars and tens of thousands of jobs each year. As a way to help create jobs, grow our economy and protect our businesses, I have introduced the Trade Secrets Protection Act of 2014. This bill will help supply American businesses, both large and small, with the tools needed to combat these destructive threats» (available at: <<http://holding.house.gov/media-center/press-releases/congressman-holding-introduces-bipartisan-trade-secrets-protection-act>>, July 29, 2014).

193 See <http://ec.europa.eu/internal_market/iprenforcement/trade_secrets/index_en.htm>.

194 See the Proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure of November 28, 2013 (COM/2013/0813 final – 2013/0402 (COD)) (available at: <http://ec.europa.eu/internal_market/iprenforcement/trade_secrets/index_en>).

It is also important to note from the outset that the protection of trade secrets does not only affect major multinational corporations¹⁹⁵, but also – and perhaps even more seriously – smaller business entities (which may have to rely on trade secrets instead of pursuing a patent filing strategy for financial reasons)¹⁹⁶.

Trade secrets are particularly vulnerable in the digital online environment in which massive amounts of data are kept on networks and in which risks of cyber attacks are common¹⁹⁷.

Under Swiss law¹⁹⁸, the protection of trade secrets results from various legal sources, which include Art. 4 lit. c¹⁹⁹ and Art. 6²⁰⁰ of the Swiss Act against Unfair Competition («SAUC»), Art. 162 («Breach of manufacturing or trade

htm>); on June 16, 2015, the European Parliament legal affairs committee approved the draft rules and a mandate to start informal talks with the Council with a view to reaching a first-reading agreement, see <<http://www.europarl.europa.eu/news/en/news-room/content/20150615IPR66493/html/Trade-secrets-freedom-of-expression-must-be-protected-say-legal-affairs-MEPs>>.

195 It being noted that the risk of trade secret misappropriation has been identified as being particularly important for companies who expand their activities at the international level, specifically in their supply chain, see the interesting (and quite alarming) report Trade Secret Theft: Managing the Growing Threat in Supply Chains (2012), available (for download) at: <<https://create.org/resource/trade-secret-theft-managing-the-growing-threat-in-supply-chains/>>.

196 See the report of WIPO in assessing the use of the IP system by SMEs, «Intellectual Property Rights and innovation in Small and Medium Sized Enterprises» (WIPO), available at: <http://www.wipo.int/export/sites/www/sme/en/documents/pdf/iprs_innovation.pdf>; see also the information provided by the WIPO SME Division on these issues, see <http://www.wipo.int/sme/en/ip_business/trade_secrets/trade_secrets.htm> and <http://www.wipo.int/?sme/en/documents/wipo_magazine/05_2002.pdf>.

197 This report will focus on the legal issues relating to the protection of trade secrets; it will consequently not analyze the criminal law issues relating to cybersecurity and cyber-attacks as such, as resulting from the relevant provisions of the Swiss Criminal Code («SCC»), which include Art. 143 SCC «Unauthorized obtaining of data» and Art. 143bis SCC «Unauthorized access to a data processing system»; for an analysis of the relevant provisions relating to cybercrimes under Swiss and comparative law, see JÉRÉMIE MÜLLER, La cybercriminalité économique au sens étroit – Analyse approfondie du droit suisse et aperçu de quelques droits étrangers, doctoral thesis, Lausanne 2012; this report will not discuss either the challenging and complex aspects of private international law that may arise in (online) trade secret misappropriation cases; on this issue, see CHRISTOPHER WADLOW, Bugs, Spies and Paparazzi: Jurisdiction over Actions for Breach of Confidence in Private International Law, European Intellectual Property Review 2008, p. 269–279; CHRISTOPHER WADLOW, Trade Secrets and the Rome II Regulation on the Law Applicable to Non-Contractual Obligations, European Intellectual Property Review 2008, p. 309–319.

198 For an analysis, see RALPH SCHLOSSER, La protection des secrets économiques in: Entreprises et propriété intellectuelle, Lausanne 2010, p. 77–109 (available at: <<http://www.kasser-schlosser.ch/pdf/Ralph%20Schlosser%20-%20La%20protection%20des%20secrets%20%C3%87co%20nomi%20ques.pdf>>).

199 «Shall be deemed to have committed an act of unfair competition, anyone who, in particular, [...] c) induces employees, agents or ancillaries to betray or pry into the manufacturing or trading secrets of their employer or principal, [...]».

200 «Shall be deemed to have committed an act of unfair competition, anyone who, in particular, exploits or discloses manufacturing or trading secrets he has discovered or of which he has obtained undue knowledge in some other manner».

secrecy»)²⁰¹ and Art. 273 of the Swiss Criminal Code («Industrial espionage»)²⁰² all of which are based on the same legal concept which has been defined by case law²⁰³ and which corresponds to the notion of «undisclosed information» resulting from Art. 39 TRIPS²⁰⁴, which is why this provision will serve as basis of the legal analysis that shall be made in the next sections²⁰⁵.

II. Art. 39 TRIPS

1. Introduction

Art. 39 para. 1 TRIPS provides that «1. In the course of ensuring effective protection against unfair competition as provided in Article 10*bis* of the Paris Convention (1967), Members shall protect undisclosed information in accordance with paragraph 2 [...]».

201 This provision provides that «[a]ny person who betrays a manufacturing or trade secret that he is under a statutory or contractual duty contract not to reveal, any person who exploits for himself or another such a betrayal, is liable on complaint to a custodial sentence not exceeding three years or to a monetary penalty».

202 This provision provides that «[a]ny person who obtains a manufacturing or trade secret in order to make it available to an external official agency, a foreign organization, a private enterprise, or the agents of any of these, or, any person who makes a manufacturing or trade secret available to an external official agency, a foreign organization, a private enterprise, or the agents of any of these, is liable to a custodial sentence [...]».

203 Swiss Federal Supreme Court, decision 6B_496/2007 of April 9, 2008, para. 5.1 (about Art. 162 SCC): «Constitue un secret, toute connaissance particulière qui n'est ni de notoriété publique ni facilement accessible et que son détenteur a un intérêt légitime à garder secrète. Par secrets commerciaux, on entend des informations qui peuvent avoir une incidence sur le résultat commercial; il peut s'agir notamment de connaissances relatives à l'organisation, au calcul des prix, à la publicité et à la production» (see also the decision of the Swiss Federal Supreme Court, decision 6B_56/2014 of December 16, 2014, para. 8.1; ATF 80 IV 22 para. 2 a; ATF 103 IV 283 para. 2b; ATF 109 IV 47 para. 5c); for an analysis, see SCHLOSSER (note 198), p. 78–81; this report will not discuss the protection of certain specific types of confidential information by other regulatory instruments, such as by regulations on banking secrecy, personal data, personality rights, etc..

204 See MARKUS R. FRICK, *Basler Kommentar UWG*, Basel 2013, N 13 ad art. 6; see also INGO MEITINGER, *Die globale Rahmenordnung für den Schutz von Geschäftsgeheimnissen im TRIPS-Abkommen der WTO und ihre Auswirkungen auf die Rechtslage in der Schweiz*, sic! 2002, p. 145–159, p. 154 (confirming that the conditions of protection as developed by Swiss case law comply with the conditions resulting from Art. 39 TRIPS); for a detailed analysis, see INGO MEITINGER, *Der Schutz von Geschäftsgeheimnissen im globalen und regionalen Wirtschaftsrecht – Stand und mögliche Entwicklungen der Rechtsharmonisierung*, Bern 2001; on the protection of know-how, see also TOBIAS MEILI, *Der Schutz von Know-how nach schweizerischem und internationalem Recht – Anpassungsbedarf aufgrund des TRIPS-Abkommens?*, Bern 2000 (this report will not specifically address the issue of know-how, which is not identical to trade secrets/undisclosed information, see e.g. SCHLOSSER (note 198), p. 81–82).

205 Certain parts of this section are derived from JACQUES DE WERRA, *International Transfer of Trade Secrets: Traps and Promises*, in: Jacques de Werra (ed.), *La protection des secrets d'affaires/The Protection of Trade Secrets*, Geneva 2013, p. 101–120.

This provision provides for the obligation to protect undisclosed information by referring to Art. 10bis of the Paris Convention (in the version of 1967)²⁰⁶. This reference to Art. 10bis of the Paris Convention is important because it confirms that the protection of confidential information is essentially anchored in unfair competition law.

At the time when the TRIPS was negotiated, voices arose against the inclusion of the protection of trade secrets on the ground that such protection did not relate to intellectual property and thus was to be kept outside of the scope of negotiation²⁰⁷. However, after relatively intensive debates, and in view of the fact that the protection is anchored in unfair competition law and that unfair competition constitutes a branch of intellectual property²⁰⁸, these objections could be overcome and as a result Art. 39 could ultimately be adopted. Given that the protection of undisclosed information is based on unfair competition law, it cannot be viewed as creating a property right on such information²⁰⁹, by contrast to traditional intellectual property rights (such as patents, copyrights and trademarks). On this basis, it is generally considered that the protection granted under Art. 39 is not enforceable *erga omnes* but applies only against certain third parties which have acted unfairly against the owner of the trade secrets²¹⁰.

From a terminological perspective, it can be noted that the terms «undisclosed information» were chosen because of their neutrality by contrast to the more common concept of «trade secrets». This choice was made because of the concern that those terms would reflect some local legal concepts about the nature and the scope of the protection²¹¹. Art. 39 TRIPS does not impose to the Member States the way how the protection shall be implemented and consequently lets them decide how such protection shall be structured²¹².

206 Art. 10bis of the Paris Convention provides:

«1) The countries of the Union are bound to assure to nationals of such countries effective protection against unfair competition.

2) Any act of competition contrary to honest practices in industrial or commercial matters constitutes an act of unfair competition».

207 See MARKUS PETER/ANDRES WIEBE, in: Jan Busche/Peter-Tobias Stoll/Andreas Wiebe (eds), TRIPS: Internationales und europäisches Recht des geistiges Eigentums: Kommentar, 2nd ed., Berlin 2013, N3 ad Art. 39; for a detailed account of the legislative history of Art. 39, see NUNO PIRES DE CARVALHO, The TRIPS Regime of Antitrust and Undisclosed Information, The Hague 2008, p. 207 seq.

208 As this results in particular from Art. 2 of the 1967 Convention Establishing the World Intellectual Property Organization (available at: <http://www.wipo.int/treaties/en/text.jsp?file_id=283854>) as pointed out by DANIEL GERVAIS, The TRIPS agreement: drafting history and analysis, 4th ed., London 2012, p. 541 footnote 758.

209 CARLOS MARIA CORREA, Trade related aspects of intellectual property rights: a commentary, Oxford 2007, p. 367 seq.; from this perspective, the terms «proprietary information» is not adequate.

210 CORREA (note 209) p. 368.

211 GERVAIS (note 208), p. 541 (noting that this terminological choice was made «to avoid referring to an expression linked to a given legal system»); see also CORREA (note 209), p. 368.

212 No specific piece of legislation is required, PIRES DE CARVALHO (note 207), p. 224.

Art. 39 para. 2 TRIPS defines the condition under which undisclosed information shall be protected. It consequently provides that:

«[n]atural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices (10) so long as such information:

- (a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
- (b) has commercial value because it is secret; and
- (c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret».

These specific conditions of protection resulting from Art. 39 para. 2 TRIPS must be carefully analyzed in the light of the new opportunities and new risks generated in the online environment.

2. *Conditions of protection*

It is necessary to analyze the definition of undisclosed information (see below a) before turning to the prohibited acts (see below b).

a. *Definition of undisclosed information*

aa. *Secrecy*

In order to be protected under Art. 39 para. 2 TRIPS, the information at issue must be secret. A piece of information is viewed as secret provided that «it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question». This wording defining the concept of secrecy was proposed by Switzerland in the first round of the TRIPS negotiations²¹³. A key element of this definition is that the information at issue must not be generally known or must not be «readily accessible», which is close to the wording of «readily ascertainable» which is used in some national regulations (such as in the US Uniform Trade Secrets Act)²¹⁴.

The formulation of Art. 39 para. 2 (a) also makes it clear that even if some individual elements of a complex body of information are known, the information as a whole can still be viewed as secret²¹⁵. The third element of Art. 39 para. 2 (a) is that the secrecy must be assessed from the perspective of the relevant informational market, i.e. of the «circles that normally deal with the kind of information

213 PIRES DE CARVAHLO (note 207), p. 231.

214 For an analysis, see PIRES DE CARVAHLO (note 207), p. 232.

215 PIRES DE CARVAHLO (note 207), p. 232.

in question». This means that a piece of information can still be secret if one competitor on the relevant market does not have access to such information, i.e. that such information is not easily ascertainable by the relevant entity²¹⁶.

By contrast, secrecy within the meaning of Art. 39 para. 2 (a), does not mean that no third party knows about the trade secrets at issue, because it is quite possible and even frequent that the relevant trade secrets are communicated to third parties (such as employees, contractual partners) who are however bound by duties of confidentiality towards the owner of such trade secrets²¹⁷.

In the digital environment, one issue which must be analyzed is whether and how the concept of accessibility (or non-accessibility) as resulting from Art. 39 para. 2 (a) TRIPS can be affected by digital data search technologies.

This issue can be illustrated by an interesting US dispute in which an executive search consulting firm specializing in the recruitment and placement of professionals for the financial services industry (Sasqua Group) sued a former employee for trade secret misappropriation of its customer information database. In that case, the court acknowledged that the information in Sasqua's database «may well have been a protectable trade secret in the early years of Sasqua's existence when greater time, energy and resources may have been necessary to acquire the level of detailed information to build and retain the business relationships at issue here»²¹⁸. The court considered however that «for good or bad, the exponential proliferation of information made available through full-blown use of the Internet and the powerful tools it provides to access such information in 2010 is a very different story»²¹⁹. In that case, the former employee (Mrs Courtney who was defendant in the proceedings together with the company under which she had started to do business) pleaded in the proceedings that «[t]he stock tool of the trade is the Internet, where information regarding prospective financial institution customers, as well as job candidates, is equally and readily available to any recruiter»²²⁰ and that «virtually all capital markets personnel have their contact information on Bloomberg, LinkedIn, Facebook or other publicly available databases, including a firm's own media advertising». The Court further held that «[t]he demonstration conducted by defendant Courtney at the hearing established that the allegedly secret information from the Sasqua database could be properly acquired or duplicated through a straightforward series of Internet searches in a drilling down exercise that likely could be duplicated by a recruiter in the executive search business for the financial services/foreign exchange industry»²²¹.

216 PIRES DE CARVAHLO (note 207), p. 233.

217 PIRES DE CARVAHLO (note 207), p. 232.

218 *Sasqua Gr., Inc. v. Courtney and Artemis*, No. CV-10-528, 2010 WL 3613855, at *22 (E.D.N.Y. Aug. 2, 2010).

219 *Ibid.*

220 *Ibid.*

221 *Ibid.*

The Court consequently decided that no trade secrets had been misappropriated in this case. On this basis, digital technologies (and particularly Internet search technologies) can lead to a reduction of the protection of trade secrets given that certain types of information which used to be secret and valuable, risk not to be qualified as trade secrets anymore because they could be easily accessed and generated by using Internet search tools and technologies. As stated by a commentator, «[...] some new technologies and trends – such as Internet search sites and the placement of once-private information online through social media – cause the scope of trade secret law to shrink»²²².

Big data technologies could potentially accentuate this trend because they make it possible to search and combine millions of individual pieces of information (which are publicly available) and process them in order to extract valuable data results. These processes can have an impact on the condition of protection of trade secrets as the condition of secrecy requires that the relevant information «is not, as a body or *in the precise configuration and assembly of its components*, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question»²²³ (italics added). The question is therefore whether big data technologies will make it possible to configure and assemble huge amounts of information so that such information could be considered as being «generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question». This may ultimately depend on the individuality or standardization of the tools that are offered by the different providers of big data technologies that will be able to generate specific outputs and confidential data for their clients so that such data could be considered to be neither «generally known» nor «readily accessible» to their competitors and to the market as a whole. It will in any case depend on the circumstances of each case and the argument of a defendant (who would be accused of trade secret misappropriation) that the relevant information would already be available on the Internet will obviously not always be successful²²⁴.

A claimant in a trade secret misappropriation action should however strictly control the pieces of information that it shall voluntarily disclose either directly or indirectly (i.e. via business and contractual partners) on the Internet because such disclosure may prevent a finding that the relevant information would be secret²²⁵.

222 ALMELING (note 186), p. 1109.

223 Art. 39 para. 2 let. a TRIPS.

224 See the decision of the Landesarbeitsgericht Rheinland-Pfalz (ref. 6 Sa 278/11) of September 16, 2011, *Zeitschrift für Datenschutz* 2012, p. 133–134 (rejecting such argument and finding that the termination of the employment for just cause because of disclosure of trade secrets was justified in this case given that the information was not available online).

225 See *PartyLite Gifts, Inc. v. Swiss Colony Occasions*, 246 Fed.Appx. 969, 973 (6th Cir. 2007) (holding that «[g]iven the apparent widespread distribution of the PartyLite magazine and lack

The dynamic interactions that are enabled by the digital environment further create new challenges for the protection of trade secrets which particularly arise with social media²²⁶. One scenario (which has led to litigation in various countries) relates to the control over social media accounts²²⁷. The issue can arise with social media accounts of a company which are managed by persons who subsequently leave the company and are not affiliated anymore with it. What shall happen with the contacts connected to such an account (i.e. followers for Twitter, contacts for LinkedIn, «friends» or «fans» for Facebook etc.)? The claim was made that such contacts should be qualified as trade secrets of the company so that the third party who would keep control over the social media accounts after leaving the company would have – allegedly – misappropriated such corporate trade secrets²²⁸. This is what was claimed in the dispute between PhoneDog and Mr Kravitz (who was previously employed by PhoneDog)²²⁹. In this case, PhoneDog alleged that Mr. Kravitz's unauthorized use of the Twitter account (and other confidential information associated with the account) after the termination of the employment agreement, have caused it to incur US \$ 340 000 in damages. To reach this calculation, PhoneDog alleged that the account generated approximately 17 000 followers, which, according to industry standards, were each valued at US \$ 2.50. Thus, PhoneDog contended that its damages amount to US\$ 42 500 (US \$ 2.50 × 17 000) for each month that Mr. Kravitz has used the account, which at the time of filing amounted to US\$ 340 000 for eight months²³⁰.

of any confidentiality protections noted on it, *combined with the relative ease in locating sales consultants via web searches*, we cannot say the district court abused its discretion in concluding the names are not a trade secret») (italics added).

226 This new environment generates interesting legal issues, for instance with respect to non-competition and non-solicitation clauses contained in an employment agreement, where an ex-employee at issue posts information about his/her new job on his/her social media account thereby reaching his/her former colleagues and clients, on this issue, see *TEKsystems, Inc. v. Hammernick*, Civ. No. 10-CV-00819, 2010 WL 1624258 (D. Minn. March 16, 2010); trademark law issues may also arise, see CLAUDIA KELLER, *Community Management, fremde Markenbotschafter und Account Squatters: markenrechtliche Herausforderungen in Social Media*, sic! 2013, p. 507–514 (available at: <https://www.sic-online.ch/fileadmin/user_upload/Sic-Online/2013/documents/507.pdf>).

227 For a discussion of this issue from the perspective of the tension between corporate trade secrets and employee mobility, see below at 2.c.

228 See *PhoneDog v. Kravitz*, No. C 11-03474 MEJ, 2012 WL 273323, at *1 (N.D. Cal. Jan. 30, 2012); *Christou v. Beatport, LLC*, 849 F. Supp. 2d 1062, 1075 (D. Colo. 2012).

229 The dispute ultimately concluded in a confidential settlement agreement between Kravitz and PhoneDog. *PhoneDog v. Kravitz*, Stipulation for Dismissal After Settlement, C 11-03474 MEJ (N.D. Cal. Jan. 8, 2013); for an analysis, see JASMINE McNEALY, *Who Owns Your Friends? PhoneDog v. Kravitz and Business Claims of Trade Secret in Social Media Information*, 39 *Rutgers Computer & Technology Law Journal* (2013), p. 30–55, available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2135601>.

230 See *PhoneDog v. Kravitz*, No. C11-03474 MEJ., 2011 U.S. Dist. LEXIS 129229 (N.D. Cal. Nov. 8, 2011).

It is however uncertain whether social media assets (and specifically social media contacts) can qualify as trade secrets knowing that social media are generally characterized by the public availability of the relevant data (because users frequently use them for the very purpose of showing and exchanging information and data with other users). This issue was relevant in another recent US case²³¹ in which the claim was made by the plaintiff (the company Cellular Accessories for Less) that it owned the LinkedIn® contacts of one of its former employee (Mr Oakes who had created another company – Trinitas) who had kept its contacts after he left the company. The Court thus had to assess whether, and how, Mr Oakes utilized LinkedIn's privacy settings in order to keep the contact list confidential. While Mr Oakes maintained that his contact list was viewable to others on LinkedIn and thus was not secret, Cellular asserted that it would not automatically be the case if Mr Oakes had his account settings set to «private». Unfortunately, neither Cellular nor Mr Oakes provided evidence to the court regarding Mr Oakes's LinkedIn privacy settings and whether his account was publicly viewable. In any case, the Court rejected the motion for summary judgment on the ground that the dispute rose issues of material fact. The dispute subsequently settled so that it remains uncertain what privacy settings were adopted and how the trade secret issue had to be decided in this case.

In terms of protection strategy, a consequence of the limits resulting from the online availability of many pieces of information (which means that the condition of secrecy would not be met), it will be important for entities wishing to control the information that they make available online to adopt other protection mechanisms, specifically contractual mechanisms, in order to prevent the misappropriation of such data. Viewed from a broader perspective, contractual protection mechanisms are and remain quite important for protecting against «screen scraping»/«database scraping» because of the limits of other sources of legal protection, as confirmed by recent case law. Reference can be made here to the recent decision of the CJEU in the *Ryanair v PR Aviation* case²³² relating to the legal protection of databases in which the Court held that, with respect to a database which is not protected either by copyright or by the *sui generis* right under the Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, the provider of such a database can impose contractual limitations on its use by third parties (without prejudice to the applicable national law). This ruling consequently confirms the importance of contractual use restrictions that can be imposed in the online environment²³³, which however presuppose that such contracts are

231 *Cellular Accessories for Less, Inc. v. Trinitas, LLC*, CV 12-06736, 2014 U.S. Dist. LEXIS 130518 (C.D. Cal. Sept. 16, 2014).

232 *Ryanair Ltd v PR Aviation BV*, Case C-30/14, decision of the CJUE of January 15, 2015.

233 See SUSAN McLEAN/MERCEDES SAMAVI, *Data for the Taking: Using Website Terms and Conditions to Combat Web Scraping*, Morrison & Foerster's Socially Aware Newsletter (March 12,

enforceable, in the sense that users of the relevant databases can be considered to have validly agreed to the conditions of use of such databases²³⁴ and that such conditions are considered as enforceable under the relevant laws²³⁵. The importance of alternative protection mechanisms (such as a contract) is equally high under Swiss law in view of the relative weakness of the protection offered by unfair competition law (and specifically by Art. 5 let. c SAUC)²³⁶.

bb. Information which has commercial value because it is secret

Art. 39 para. 2 (b) TRIPS provides that the information at issue must have «commercial value because it is secret». This provision contains two sub-conditions, which are that the information must have commercial value and that such commercial value is due to the fact that it is secret²³⁷.

The concept of commercial value should not be interpreted too narrowly. On this basis, it should be admitted that trade secrets protection can also be enforced by non-commercial entities, the only condition being that such protection is sought for the purpose of protecting «competing advantages»²³⁸. From this perspective, it can be acknowledged that «commercial value» means «competitive value»²³⁹, which consequently implies that the information provides a competing advantage to its beneficiary. In terms of burden of proof, the value

2015), available at: <<http://www.sociallyawareblog.com/2015/03/12/data-for-the-taking-usin-g-website-terms-and-conditions-to-combat-web-scraping/>>.

234 This contractual issue requires to assess to what extent the general terms and conditions have been validly accepted by the user, which must be analyzed under the relevant law; a separate issue (which bears a certain similarity) is whether a choice of court clause contained in general terms and conditions of one contracting party can be held to have been validly accepted by the other contracting party on the basis of a reference made in an email to the general terms and conditions; this was admitted in a recent case decided by the Swiss Federal Supreme Court in which the parties communicated by email, ATF 139 III 345 para. 4.4 (about Art. 23 para. 1 let. a – relating to the conditions of validity of prorogation clauses – of the Convention on the jurisdiction and the recognition and enforcement of judgments in civil and commercial matters of October 30, 2007 (Lugano Convention)); the issue can also arise for arbitration clauses contained in online agreements, see e.g. Kevin Khoa Nguyen v. Barnes & Noble Inc., 2014 U.S. App. LEXIS 15868 (9th Cir. 2014).

235 By way of example, the Court of Milan recently ruled that Ryanair's refusal to grant access to its database to the online travel agency Viaggiare S.r.l. amounted to an abuse of dominant position in the downstream market of information and intermediation on flights, decision of June 4, 2013 of the court of Milan in the case Viaggiare S.r.l. vs Ryanair Ltd, available at: <http://www.opic.it/index.php?option=com_docman&task=doc_details&gid=494&Itemid=60>.

236 See ATF 131 III 384; ATF 134 II 166.

237 PIRES DE CARVALHO (note 207), p. 233 ss.

238 PIRES DE CARVALHO (note 207), p. 235; reference can also be made to a recent US case *New Hampshire Right to Life v. U.S. Dep't of Health & Human Servs.*, 778 F.3d 43 (1st Cir. 2015), in which the Court held that the entity which was concerned (i.e. Planned Parenthood, which is a non-profit organization), could possess confidential, commercial information, and protect it from disclosure under the US Freedom of Information Act («FOIA»).

239 PIRES DE CARVALHO (note 207), p. 235.

does not need to be strictly established given that such value can be actual or potential²⁴⁰.

The second element of the definition of Art. 39 para. 2 (b) TRIPS is that the secret shall extract value from the fact that it is secret²⁴¹. This means that the value of the secret information must be negatively affected because of its disclosure, acquisition or use by a third party²⁴².

cc. Reasonable steps to keep the information secret

Art. 39 para. 2 (c) TRIPS further provides that the protection of the confidential information can only be available provided that the information at issue «has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret».

This provision sets an objective standard with respect to the measures which are to be taken by the person controlling the confidential information in order to claim the protection under Art. 39 TRIPS. In other words, the protection of confidential information can only be claimed if and to the extent that the owner of such information has taken reasonable measures to keep it secret «under the circumstances». One key aspect of this provision results from the standard of reasonableness to which it refers. This means that the owner is not supposed to take all imaginable measures that could potentially be taken²⁴³.

This also means that not all types of confidential information require the same measures of protection in order to deserve legal protection. Quite to the contrary, the standard of reasonableness depends on the nature and commercial value of the secrecy at issue. From this perspective, this provision introduces a test of proportionality²⁴⁴.

The intangible nature of trade secrets (which is perhaps the most intangible type of all intellectual property rights) sometimes make it difficult to enforce their protection in certain circumstances. Even if the protection of trade secrets does not depend on the taking of any formal official step by the holder of such secrets²⁴⁵ so that the perception may arise that trade secrets would be easier to protect, their efficient protection unavoidably requires a very high level of diligence, which is sometimes neglected. Case law indeed teaches that many

240 PIRES DE CARVALHO (note 207), p. 233.

241 PIRES DE CARVALHO (note 207), p. 235.

242 PIRES DE CARVALHO (note 207), p. 235–236.

243 VICTORIA A. CUNDIFF, Reasonable Measures to Protect Trade Secrets in a Digital Environment, IDEA – The Intellectual Property Law Review 2009, vol. 49, p. 359–410, p. 363, available at: <http://ipmall.info/hosted_resources/IDEA/idea-vol49-no-3-cundiff.pdf>: «While careful efforts to preserve secrecy are required of trade secret owners, the owner is not required to take every *conceivable* measure to maintain secrecy. The law does not require «super-reasonable» measures to maintain secrecy because doing so would require over-investment in protection, potentially reducing innovation and creating inefficiencies, [...]».

244 PIRES DE CARVALHO (note 207), p. 237.

245 By contrast to patent protection which presupposes the filing of a patent application.

claims of alleged misappropriation of trade secrets fail because the claimant was not sufficiently diligent in the first place in taking the required (contractual) measures of protection.

Case law first confirms the obvious risk of disclosure of trade secrets to potential licensees/business partners before a formal agreement has been entered into. If the negotiations subsequently fail, the party having – somehow irresponsibly – disclosed its trade secrets will have a hard time enforcing a claim of misappropriation of trade secrets: the courts will likely find that the disclosed information were not trade secrets because of the lack of measure of protection taken in order to keep them confidential (which is a standard condition of protection of trade secrets)²⁴⁶.

The digital online environment makes it necessary to assess anew the concept of «reasonable steps» (pursuant to the wording of Art. 39 para. 2 (c) TRIPS) that shall be expected in order to preserve the secrecy and confidentiality of the relevant trade secrets²⁴⁷.

Digital access to the relevant information must be efficiently controlled, for which digital access protection mechanisms must be adopted²⁴⁸.

246 See *U.S. Plywood Corp. v. General Plywood Corp.*, 370 F.2d 500, 152 U.S.P.Q. 80 (6th Cir. 1966) (rejecting the claim because the claimant did not make «any effort at [...] securing an agreement for confidentiality»).

247 See CUNDIF (note 243), *passim*; see generally ELIZABETH A. ROWE, Rethinking «Reasonable Efforts» to Protect Trade Secrets in a Digital World (2008), available at: <http://works.bepress.com/elizabeth_rowe/2/>; an example of negligent conduct (i.e. of absence of reasonable steps) was recently given by the French TV channel TV5 Monde which shortly after the highly-media-tized cyberattack that it suffered apparently made visible its passwords to its social media on a TV report, see «France TV5Monde passwords seen on cyber-attack TV report», BBC (April 10, 2015), available at: <<http://www.bbc.com/news/world-europe-32248779>>.

248 See e.g., *Four Seasons Hotels & Resorts B.V. v. Consorcio Barr, S.A.*, 267 F. Supp. 2d 1268, 1301 (S.D. Fla. 2003) (finding that the plaintiff could benefit from the protection of its trade secrets because it had relied on a secure VPN solution provider offered by an external third party so that the defendant – who was bound by a license agreement with the plaintiff – who unduly accessed trade secrets – i.e. guest profiles – was found in breach of the Uniform Trade Secrets Act, as codified at Fla. Stat. §§ 688.001–688.009 because of its undue access to Four Seasons' detailed customer profiles, by espionage through electronic means); see also *Paz Systems, Inc. v. The Dakota Group Corp.*, 514 F.Supp.2d 402, 406 (E.D.N.Y.2007) (employer's computer network was stored in a building protected by both commercial locks, passwords and an alarm system, including motion detectors); *Wrap-N-Pack, Inc. v. Eisenberg*, No. 04-cv-4887, 2007 WL 952069, at *9 (E.D.N.Y. March 29, 2007) (company implemented significant safeguards to protect information by requiring user identification and password; installing firewalls and security software that prevented salesmen from accessing any information regarding other salesmen's customers; installing passwords and restrictions of all laptop computers; circulating policy and procedure manual containing a code of conduct defining disclosure of confidential information as unacceptable behavior; pursuing litigation to prevent the threatened disclosure of confidential information); *B.U.S.A. Corp. v. Ecogloves, Inc.*, No.05 CIV. 9988, 2006 WL 3302841, at *4 (S.D.N.Y. Jan. 31, 2006) («plaintiffs took appropriate measures, such as locking files and using computer passwords, to protect the contact information»); by contrast, in *Sasqua Group, Inc. v. Courtney*, No. CV 10-528, 2010 WL 3613855 at *19 (E.D.N.Y. Aug. 2, 2010), the Court held that «Sasqua failed to take even basic steps to protect the secrecy of the information contained in its database – the very same information Tors [the manager of the plaintiff] refers to as «the life-

The storage of trade secrets on cloud services can also be problematic to the extent that it may be considered that the fact of using such remote storage capacities may imply that no reasonable measures of protection have been taken, also because the relevant cloud service agreements frequently do not provide for an obligation of confidentiality which could have served as a basis for admitting that reasonable measures would have been taken²⁴⁹.

Prohibiting the disclosure of trade secrets which would be posted on the Internet has raised constitutional concerns in the United States in the sense that restraining orders/injunctions were perceived as potentially preventing the diffusion of socially relevant information thereby leading to a conflict between trade secrets and constitutional rights (particularly free speech). In one early Internet disclosure case, the court however expressed concern that not enjoining the defendant from posting the relevant confidential information on the Internet would «encourage misappropriators of trade secrets to post the fruits of their wrongdoing on the Internet as quickly as possible and as widely as possible thereby destroying a trade secret forever. Such a holding would not be prudent in this age of the Internet»²⁵⁰. The issue is therefore to assess how the respective rights should be balanced²⁵¹.

The making available of trade secrets on the Internet shall not necessarily prevent the granting of injunctive relief if the posting is «sufficiently obscure or transient or otherwise limited so that it does not become generally known to relevant people, *i.e.*, potential competitors or other persons to whom the information would have some economic value»²⁵². It may be wondered whether such statement still holds true today. The reason is that Internet storage and

blood of Sasqua's business»); see also *Boston Laser, Inc. v. Zu*, No. 3:07-CV-0791, 2007 WL 2973663, at *10, *12 (N.D.N.Y. Sept. 21, 2007) (finding that plaintiff had not taken reasonable measures to preserve secrecy where, among other things, «the computer network on which such matters are digitally stored is generally not even password protected beyond the log-in process»).

249 See SHARON K. SANDEEN, *Lost in the Cloud: Information Flows and the Implications of Cloud Computing for Trade Secret Protection*, 19 *Virginia Journal of Law & Technology* (2014), p. 1–103, p. 56 (available at: <http://www.vjolt.net/vol19/issue1/v19i1_1-Sandeen.pdf>): «Without the existence of either an express or implied confidential relationship with its cloud storage service, a company that pursues trade secret misappropriation claims for information that is (or has been) stored in the cloud is likely to confront defense arguments that such information is no longer (or never has been) entitled to trade secret protection due to the fact that it was stored in the cloud. In this regard, the defendant will argue that it was not reasonable to store information in the cloud without first securing an express promise of confidentiality».

250 *DVD Copy Control Ass'n v. McLaughlin*, No. CV 786804, 2000 WL 48512, at *3 (Cal. Super. Ct. Jan. 21, 2000).

251 See PAMELA SAMUELSON, *First Amendment Defenses in Trade Secrecy Cases*, in: Rochelle C. Dreyfuss/Katherine J. Strandburg (ed.), *The Law and Theory of Trade Secrecy. A Handbook of Contemporary Research*, Cheltenham (UK)/Northampton(USA) 2011, p. 269–297; see also DAVID GREENE, *Trade Secrets, the First Amendment, and the Challenges of the Internet Age*, 23 *Hastings Communications and Entertainment Law Journal* (2001), p. 537–561.

252 See *DVD Copy Control Ass'n v. Bunner*, 10 Cal. Rptr. 3d 185, 192–93 (Cal. Ct. App. 2004).

search technologies may make it more difficult to consider that a post on the Internet could be considered as being «sufficiently obscure or transient or otherwise limited» given the (high) speed at which information can be shared and transmitted on online (social) networks. On this basis, it will be quite difficult to consider that a piece of (confidential) information which would have been made available on the Internet could be subsequently entirely removed. For this reason, proposals have been formulated in order to make it possible for trade secret owners to react faster and request and obtain the taking down of the relevant information without having to wait for a court order²⁵³.

b. Prohibited acts

As provided by Art. 39 para. 1 TRIPS, the beneficiaries of the protection have the right to prevent «information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices».

This wording evidences that three different and mutually independent acts can constitute a misappropriation of confidential information: the disclosure, the acquisition and the use of the confidential information²⁵⁴. In addition, such acts must have been performed «in a manner contrary to honest commercial practices». In this respect, Art. 39 para. 1 TRIPS contains a footnote which defines the concept of the contrariety to «honest commercial practices» by providing that «[for] the purpose of this provision, <a manner contrary to honest commercial practices> shall mean at least practices such as breach of contract, breach of confidence and inducement to breach, and includes the acquisition of undisclosed information by third parties who knew, or were grossly negligent in failing to know, that such practices were involved in the acquisition»²⁵⁵. This definition of the concept of contrariety to honest commercial practices implies the adoption of a subjective standard of analysis (i.e. a standard based on a finding of bad faith)²⁵⁶.

The first prohibited act which is mentioned in Art. 39 TRIPS is unsurprisingly the disclosure of the relevant information at issue. It is indeed quite clear that the protection of confidential information must include a protection against the unauthorized disclosure of a trade secret.

253 ELIZABETH A. ROWE, *Introducing a Takedown for Trade Secrets on the Internet*, 2007 *Wisconsin Law Review* (2007), p. 1041–1089, available at: <<http://scholarship.law.ufl.edu/facultypub/63>> (suggesting adoption of procedures similar to those afforded to copyright owners under the Digital Millennium Copyright Act).

254 PIRES DE CARVALHO (note 207), p. 229.

255 Which is footnote 10 of the TRIPS agreement.

256 PIRES DE CARVALHO (note 207), p. 231 footnote 473 citing WTO document IP/Q3/AUS/1 of October 22, 1997, p. 9 (referring to a «broader principle of equity concerned with ensuring that persons do not suffer from an exercise of bad faith on the part of another»).

It is obvious that Internet offers a unique platform for global disclosure and for worldwide visibility of leaked trade secrets²⁵⁷, so that protection is requested against such undue disclosure.

The other types of acts referred to in Art. 39 para. 2 are the acquisition and the use of confidential information. It is important to note in this respect that Art. 39 TRIPS alternatively refers to the acquisition or the use of confidential information, which means that the acquisition by itself can be sufficient for finding a violation under Art. 39 TRIPS, irrespective of a potential use of the confidential information by the person which has unlawfully acquired it (or by a third party which would have obtained such information). This is important from a practical perspective because it will frequently be quite difficult to prove the effective use of the confidential information.

In the digital environment, the question has arisen as to whether an act of access was sufficient to be considered as a misappropriation²⁵⁸. It should however be admitted that access can be sufficient even in the absence of showing of disclosure to or use by a third party (potentially the new employer of an employee taking/saving confidential information on a not work-related external data carrier)²⁵⁹. Certain regulations on trade secrets specifically address computer-related acts of misappropriation. This is specifically the case of the Virginia Uniform Trade Secrets Act which provides that misappropriation through acquisition occurs when a person «knows or has reasons to know that the trade secret was acquired by improper means», whereby «improper means» includes «theft, bribery, misrepresentation, *use of a computer or computer network with-*

257 See O'Grady v. Superior Court, 139 Cal. App. 4th, 1423, 1432 (Cal. App. Ct. 2006) (release on the Internet of Apple's «secret plans to release a device that would facilitate the creation of digital live sound recordings on Apple computers»); Ford Motor Co. v. Lane, 67 F. Supp. 2d 745, 746–47 (E.D. Mich. 1999) (photos of upcoming Ford products leaked onto the Internet).

258 Kelly Servs., Inc. v. Greene, 535 F. Supp. 2d 180, 186 & n. 8 (D. Me. 2008) (finding that the fact that defendant transferred files to a USB drive prior to resignation did not establish misappropriation in face of sworn statements that she did not retain protected information and in absence of proof that she had used any of the information).

259 See Marsteller v. ECS Federal, Inc., No. 1:13-cv-593, 2013 U.S. Dist. LEXIS 126927 (E.D. Va. September 5, 2013): in this case, the plaintiff's claim (ECS) was based on the fact that the defendant (Mrs Masteller, who was one of its employees) transferred and retained internal documents belonging to ECS outside the scope of the permitted use provided by her employment (she transferred proprietary documents belonging to ECS to an external storage device); see also Bridgetree, Inc. v. Red F Marketing, LLC, No. 10-228, 2013 U.S. Dist. LEXIS 15372 (W.D.N.C. Feb. 5, 2013) at *7 holding that «[t]estimony showed that Mr. Li acquired trade secrets upon his departure from Plaintiff through the downloading of information from Plaintiff's servers to a one-terabyte flash drive owned by Mr. Li and retained by him following his resignation. Spoliation of evidence –including the deletion of information from Mr. Li's computer he used while employed with Plaintiff, along with the discarding of a personal family computer he used for work while employed by Plaintiff – provides circumstantial evidence to permit the jury to draw an adverse inference of misappropriation through the «acquisition» of compilation source codes».

out authority, breach of a duty or inducement of a breach of duty to maintain secrecy, or espionage through electronic or other means» (italics added)²⁶⁰.

c. Balance between employee mobility and corporate trade secrets

The protection of corporate trade secrets shall not affect the employees' ability to be mobile and to change job. It is consequently important to distinguish the corporate trade secrets (which should not be misappropriated) from the personal skills and talent and personal information of the relevant employees (from which the new employer can benefit).

An interesting issue which may arise in this respect and which illustrates the potential tension between corporate trade secrets and employee mobility relates to the control of social media account and contacts²⁶¹. The balance between these two conflicting interests is complex and will depend on the circumstances of the case, which can be illustrated as follows:

If, by way of example, a company instructs an employee to open and manage a corporate Twitter account (that shall ideally reflect the name/trademark of the company), the application of the rules governing employment contracts could imply that the company shall be entitled to control and keep the social media account and the contacts associated to it even after the termination of the employment contract²⁶². Subject to the existence of detailed contractual provisions (potentially contained in corporate social media policies) which would specifically address this issue, this outcome could flow from the duty of loyalty and from the obligation of the employee to hand-over the benefits and the work produced in the course of his contractual activities (as provided by Art. 321b of the Swiss Code of Obligations)²⁶³.

The issue can become more complex if the company requests an employee to open a LinkedIn account to be used for a corporate purpose. In such a case, the employee will indeed use the social network in order to build his/her own professional network of contacts so that he/she could be entitled to keep control over these contacts even after the termination of the employment relationship²⁶⁴. The scenario will still be different if the social media account has been

²⁶⁰ § 59.1-336, Code of Virginia (Title 59.1 – Trade and Commerce. Chapter Uniform Trade Secrets Act), available at: <<http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+59.1-336>>.

²⁶¹ COURTNEY J. MITCHELL, Keep Your Friends Close: A Framework for Addressing Rights to Social Media Contacts, 67 Vanderbilt Law Review (2014), p. 1459–1495, available at: <<http://www.vanderbiltlawreview.org/content/articles/2014/10/Keep-Your-Friends-Close-A-Framework-for-Addressing-Rights-to-Social-Media-Contacts.pdf>>.

²⁶² For a real-life illustration, see the PhoneDog v Kravitz dispute (note 230).

²⁶³ See MICHÈLE STUTZ/ALEXANDRA GEIGER-STEINER, Arbeitsrechtliche Fragen rum um Social Media, Revue de l'Avocat/Anwaltsrevue 2013, p. 212–216, p. 215; for a general analysis of social media law, see Social Media und Recht in der Schweiz (Oliver Staffelbach/Claudia Keller eds), Zurich 2015.

²⁶⁴ STUTZ/GEIGER-STEINER (note 263), p. 215–216; this is precisely what was at issue in the US case Eagle v. Morgan, CIV 11-4303, 2012 WL 4739436, at *9 (E.D. Pa. Oct. 4, 2012); for other

opened by a third party with no relationship with the relevant company (and not by an employee), who can potentially be a fan of the company's products and brand, and if the company subsequently takes control over the social media account. Unless this is adequately managed, the risk is that this may end up in litigation, which is what happened about the Facebook page of «Ferrari» (<http://www.facebook.com/ferrari>)²⁶⁵, which was created by a Geneva-based fan (and driver) and which led to multiple and complex litigation in Geneva and abroad (which are still pending)²⁶⁶.

The multifaceted nature of social media and online social interactions, which combine corporate and personal interests as well as the professional and personal life of the users, makes it difficult to establish bright line rules defining the allocation of rights and controls over the potentially very valuable «digital assets» that are generated by users online and that may constitute trade secrets.

The complexity of those legal issues and of the disputes which may ensue also result from their international nature (which can raise thorny issues of jurisdiction and governing law) and from the interactions between different sources of regulations, whereby the rules and practices adopted – i.e. imposed²⁶⁷ – by social media platforms will unquestionably play a prominent role in this context.

This triggers the question whether social media should be regulated by specific laws. In its report published in October 2013, the Swiss Federal Council decided that this was not needed at this stage, also in light of on-going regulatory projects (particularly data protection) which may affect social media²⁶⁸.

cases (coming from the UK) dealing with the control of contacts of a LinkedIn account and of LinkedIn groups respectively, see *Hays Specialist Recruitment (Holdings) Ltd & Anor v Ions & Anor* [2008] EWHC 745 (Ch) (16 April 2008) and *Whitmar Publications Ltd v Gamage & Ors* [2013] EWHC 1881 (Ch) (04 July 2013).

265 The fans of the Facebook page have grown from half a million (in 2009) to more than 16 million as of today.

266 See STEPHANIE BODONI/ANDY HOFFMAN, *Ferrari Fights 21-Year-Old Racer for Facebook Page Control* (March 27, 2014), available at: <http://www.bloomberg.com/news/articles/2014-03-27/ferrari-fights-21-year-old-racer-for-control-of-facebook-page>; a complaint was recently filed (October 14, 2014) before the Superior Court of the State of California in and for the County of San Mateo in the case *Olivier Wasem & Sammy Wasem v. Facebook, Inc. & Ferrari S.p.A.*, Case No. CIV-530869 (available at: <http://pdfserver.amlaw.com/ca/WasemvFerrari.pdf>).

267 As they result from unilaterally imposed terms and conditions that users have to accept in order to join the social media platforms, or that complainants (even if they are not users and are thus not bound by the contract relating to the use of the platforms) have to use if they want to complain about certain abusive practices committed on those social media platforms.

268 See the press release «No special law for social networks» (October 9, 2013) available at: <https://www.news.admin.ch/message/index.html?lang=en&msg-id=50504>; the report of the Federal Council (October 9, 2013): *Legal Basis for Social Media*, Report of the Federal Council in Fulfilment of the Amherd Postulate 11.3912 of 29 September 2011, is available at: <http://www.bakom.admin.ch/themen/infosociety/04837/index.html?lang=en>; this report which essentially focuses on the protection of the interests and rights of individuals on social media is of limited relevance here, given that it does not discuss issues of patents and trade secrets (it simply mentions – without in depth analysis – the issue of copyright on social media).

It is interesting to note that regulations have been adopted in certain foreign countries in order to address certain aspects of social media. This is particularly the case of US regulations (either draft regulations or already in force) which prevent employers from accessing personal social media accounts of their employees under certain circumstances²⁶⁹. These regulations remain difficult to apply particularly because they do not address and solve the difficult delimitation (discussed above) between personal social media account and corporate accounts. By way of illustration, a Californian regulation (California Assembly Bill AB1844) which was passed on September 27, 2012²⁷⁰ provides that (sec. 980.) «[a]n employer shall not require or request an employee or applicant for employment to do any of the following: (1) Disclose a username or password for the purpose of accessing personal social media [...]»²⁷¹ but does not precisely define what shall constitute a «personal social media».

This shows that regulating social media remains quite difficult so that the prudent position of the Swiss Federal Council appears appropriate.

Another issue which arises in this context relates to the potential liability of the new employer for the misappropriation of trade secrets in the hypothesis where an ex-employee of a competing team communicates those secrets to his new employer after being hired. It should be reminded in this respect that footnote 10 of Art. 39 TRIPS provides that an illicit misappropriation can occur with respect to «the acquisition of undisclosed information by third parties *who knew, or were grossly negligent in failing to know*, that such practices were involved in the acquisition» (italics added). On this basis, the standard is whether the new employer knew or was grossly negligent in failing to know that its employee did not behave according to «honest commercial practices» (which is the standard under Art. 39 para. 2 TRIPS) by potentially breaching his/her duties of confidentiality towards his/her ex-employer.

In the information age, it will be essential for a new employer to ensure – as part of its standard hiring practices – that the new employee about to be hired does not bring along corporate trade secrets from his/her previous job on digital data carriers (e.g. computer, external hard drive, USB stick, cloud service sto-

269 See the list of State regulations at: <<http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords.aspx>>.

270 Available at: <http://www.leginfo.ca.gov/pub/11-12/bill/asm/ab_1801-1850/ab_1844_bill_20120927_chaptered.html>.

271 For a critical comment of the California regulation, see ERIC GOLDMAN, Big Problems in California's New Law Restricting Employers' Access to Employees' Online Accounts (September 29, 2012), available at: <<http://www.forbes.com/sites/ericgoldman/2012/09/28/big-problems-in-californias-new-law-restricting-employers-access-to-employees-online-accounts/>>), who considers that «the law assumes that social media accounts have only two states: personal or not-personal. Instead, social media accounts fit along a continuum where the endpoints are (1) completely personal, and (2) completely business-related – but many employees' social media accounts (narrowly construed, ignoring the statutory over breadth problem) fit somewhere in between those two endpoints. Indeed, employers and employees routinely disagree about whether or not a social media account was personal or business-related».

rage capacities) and does not use them in any manner on the new job. From this perspective, a formal agreement to be signed at the time of hiring is recommended.

Reference can be made to an interesting US decision in which the defendant, (Mr Botticella) who was an employee of Bimbo Bakeries USA (the plaintiff) where he was «one of the only seven people [within Bimbo] who possessed all of the knowledge necessary to replicate independently Bimbo's popular line of Thomas' English Muffins, including the secret behind the muffin's unique «nooks and crannies» texture»²⁷², had taken confidential information and documents before leaving his job for a competitor in the baking industry (Hostess Brands). It was established (on the basis of a report of a computer forensic expert) that Mr Botticella had electronically «accessed a number of confidential documents during the final weeks of Botticella's employment at Bimbo»²⁷³ and that «a person logging in as Botticella had accessed twelve files within a span of thirteen seconds on January 13, 2010, Botticella's last day at Bimbo» and that «[s]ignificantly this access occurred minutes after the phone call in which Botticella finally disclosed to Bimbo his plans to work for Hostess and Bimbo told him to cease working for it»²⁷⁴. It was established that these documents were highly sensitive²⁷⁵ for which Mr Botticella did not give any plausible explanation²⁷⁶. The new employer (Hostess) had Mr Botticella sign an agreement for the purpose of avoiding (or at least reducing) the risk for Hostess to be found liable for misappropriation of trade secrets²⁷⁷.

272 Bimbo Bakeries USA, Inc. v. Botticella, 613 F.3d 102 (3d Cir. 2010), at *105.

273 Bimbo Bakeries USA, Inc. v. Botticella, 613 F.3d 102 (3d Cir. 2010), at *107.

274 *Ibid.*

275 They included (as established by the District Court) «Bimbo's cost-reduction strategies, product launch dates, anticipated plant and line closures, labor contract information, production strengths and weaknesses of many Bimbo bakeries, and the cost structure for individual products by brand», Bimbo Bakeries USA, Inc. v. Botticella, No.10-0194, 2010 WL 571774 (E.D.Pa. Feb.9, 2010), at *7.

276 The Court of Appeal stated (Bimbo Bakeries USA, Inc. v. Botticella, 613 F.3d 102 (3d Cir. 2010), at *108) that Mr Botticella «maintained that he had done so [i.e. to copy files periodically from his laptop to external storage devices] only to practice his computer skills in preparation for his new position at Hostess. Despite an earlier denial, he eventually admitted to conducting such «practice» exercises in January 2010. The District Court found that Botticella's explanation of his use of the laptop computer and the external devices was «confusing at best» and «not credible.» *Bimbo Bakeries*, 2010 WL 571774, at *6».

277 The document entitled «Acknowledgment and Representation Form» had the following content (Bimbo Bakeries USA, Inc. v. Botticella, 613 F.3d 102 (3d Cir. 2010), at *106): «I acknowledge that [Hostess – the new employer] has advised me that it is not interested in, nor does it want, any confidential information or trade secrets or other proprietary information that I may have acquired through any prior employment or business relationship, including without limitation any information or «know-how» related to the manufacturing of Thomas brand products. I further acknowledge that I have not previously, and will not in the future, disclose to Hostess any confidential or proprietary information belonging to any previous employer. Specifically, I acknowledge that Hostess has instructed me not to disclose to it or to use in the course of any job for it that I may be [sic] have at any time, any confidential or proprietary information belonging

III. Conclusion

In the information age in which more and more confidential corporate data are stored and transmitted digitally and in which data breaches have unfortunately become a common phenomenon, the protection of trade secrets is of vital importance. This growing importance is reflected in the dynamic regulatory activity which aims at improving and harmonizing their protection in various parts of the world (and specifically in the European Union).

The protection of trade secrets particularly requires that the relevant persons and entities which control them shall be and remain aware of the reasonable measures that they are supposed to take in order to protect their intangible assets. They consequently have to use technology in order to protect them and regularly adapt the measures to an ever changing technological environment. In the digital environment, the protection of trade secrets depends on technological tools. Technology can assist in various ways: it can help in building digital fences (in order to avoid or at least minimize the risks of data breaches and misappropriation of trade secrets). It can also help once a data breach has occurred and once a misappropriation has been committed by helping to track and identify the cause of potential data breaches and thus help identify the sources of data leakages (with the assistance of computer forensic experts). In addition, the growing availability of online data constitutes a challenge for the protection of trade secrets: what was potentially secret and was not readily accessible in the past can now become accessible thanks to powerful online data search and data processing technologies. As a result, the digital environment also affects the very concept of secrecy.

D. Lessons and perspectives

What lessons can be learnt from these developments and what perspectives do they open for the future? The following four points can be formulated:

1. There is a need to re-conceptualize certain legal concepts in the Internet era. The online availability of massive amounts of data which can be structured in increasingly sophisticated manners can affect a number of legal concepts in many different legal fields. This is particularly the case in patent law and in the law of trade secrets: under what conditions can a document available online be considered as having been «made available to the public»²⁷⁸ (under patent law), or as being not «generally known» or «readily accessible»²⁷⁹ (under the law of

to any previous employer. I represent that I have and will not bring to Hostess'[s] work place, use for the benefit of, or in any way share with Hostess any confidential or proprietary information belonging to any previous employer [...]».

²⁷⁸ Art. 7 para. 2 SPA; Art. 54 para. 2 EPC.

²⁷⁹ Art. 39 para. 2 (a) TRIPS.

trade secrets), is not undebated today and will be of major importance in the future. This consequently requires to reassess the legal notions of public availability and of secrecy in the information age.

The standards for protecting confidential information will also need to be adapted in the online environment. What «reasonable steps»²⁸⁰ to keep a piece of information confidential shall be expected in order to benefit from the legal protection? What measures can be viewed as «reasonable» at a time where major cyber-attacks make more and more victims and where cybersecurity costs are booming? How shall the standard of reasonableness be adapted over time in view of the light-speed development of (content protecting as well as hacking) technologies? Under what circumstances can the intentional online leakage of a patent-related piece of information (before the relevant patent application has been filed) be considered as «an evident abuse»²⁸¹ under patent law?

The need to reconsider certain legal standards in the information age does not mean that they have to be fully reinvented. These standards should rather emerge and be derived from the experience and hindsight gained from the existing legal system, and shall specifically result from a transdisciplinary approach because it appears that certain legal issues arise in similar terms in different legal fields. By way of example, the standard of reasonableness as a condition of protection of trade secrets can be compared to the efficiency of technological protection measures under copyright law. It is therefore important that the legal system in its entirety develops and adapts to the online environment in a coherent way. In this respect, it can be expected that the legal system shall be and remain technology neutral in the sense that the law shall apply irrespective of the technology, i.e. the law shall not be based/focused on a technological solution to the exclusion of other technologies²⁸²; the law shall not dictate which technology shall be used in order to meet the condition of reasonableness of the protection measures, in order to benefit from the protection of trade secrets. It must however – and conversely – also be expected that one technological issue shall as a matter of principle be treated similarly by different laws. By way of example, the act of circumventing a technological access protection measure and of committing a data breach shall be treated as coherently and similarly as possible under the different relevant laws. As discussed above, one condition of protection is that the technological access protection measure shall be effective (i.e. that it cannot be too easily circumvented). If such a protection mechanism is not effective, there shall be no sanction against such act under the relevant laws (particularly trade secret law, because no reasonable measures of protection would have been taken, and

280 Art. 39 para. 2 (c) TRIPS.

281 Art. 7b (b) SPA; Art. 55 EPC para. 1.

282 For copyright law, see ATF 140 III 616, para. 3.4.1: «Die Befugnis zum Eigengebrauch ist, wie grundsätzlich das ganze Urheberrechtsgesetz, technologieneutral ausgestaltet».

copyright law, because the protection mechanism would not be sufficiently effective). In this sense, a technological act (e.g. the act of circumventing) shall be treated similarly under the different relevant laws and shall consequently be treated without unjustified discrimination by the different laws: technological acts shall be legally neutral. In sum, the law should be technology neutral, but the technology should also conversely be legally neutral.

2. The information age is characterized by the free circulation of knowledge and information. This implies that measures shall be taken in order to promote the *voluntary*²⁸³ communication and exchange of information which can generally be fostered by the conclusion of contracts. This in turn means that intellectual property transactions, as transactions by which the use of intellectual property assets is enabled, shall be facilitated and that intellectual property transactions costs shall consequently be reduced²⁸⁴.

In this respect, the global debate surrounding the conditions of FRAND licensing of standard essential patents (SEPs), and the very high transactions costs which are presently caused by the negotiation and frequent litigation about FRAND licensing, show that global licensing standards need to be established both in terms of the substantive elements of a license agreement (i.e. what shall fair, reasonable and non-discriminatory licensing terms and conditions mean) and of the procedural elements of licensing negotiations (i.e. how shall FRAND licenses be negotiated and how FRAND disputes shall be solved). Global licensing standards are of key relevance for ensuring that information can and shall remain equally accessible to (mobile) Internet users at the global level without discrimination and excessive costs which may result from an unlimited enforceability of SEPs against technology implementers.

3. In the information age, legal standards are strongly influenced by technological standards. The definition of the standard of care and of diligence that shall be expected for protecting online confidential information from unauthorized misappropriation will also be established by reference to the nature and efficiency of technological mechanisms that have been put in place in order to prevent the unauthorized access to such confidential information. The legal standards applicable to analyze the substantive validity of a patent in terms of novelty and non-obviousness will depend on whether the relevant invention was included in the online state of the art or could be easily deducted from it thanks to the use of online search engines, big data and artificial intelligence technologies.

283 As discussed above (see point 1), the *involuntary* online disclosure of information and the conditions under which such unauthorized disclosure can be legally relevant are a different issue.

284 See RICHARD A. POSNER, Transaction Costs and Antitrust Concerns in the Licensing of Intellectual Property, 4 J. Marshall Review of Intellectual Property Law (2005), p. 325–335, p. 327 (available at: <<http://repository.jmls.edu/ripl/vol4/iss3/1/>>) (stating that «an important focus of legal reform should be on means of reducing intellectual property transaction costs [...]»).

While the impact of technology on the law is obviously not a new phenomenon, what is new is the growing importance of technological tools – and specifically massive and intelligent data processing tools and technologies – in defining the contours of the law, which is particularly true for intellectual property law (and specifically patent law and trade secret law). The use of smart data processing technologies could particularly have an impact on the condition of non-obviousness by making it more difficult to meet this condition, because it could sooner or later be requested from the hypothetical «person skilled in the art», who is at the core of the patent system, to use these sophisticated data processing technologies, thereby provoking the risk that the condition of non-obviousness would not be met because the invention at issue would be considered to obviously result from a combination of different sources of prior art. In a similar way (beyond patent and trade secrets but still within the field of intellectual property), Internet search engines shall not be relied upon as the primary source or even as the exclusive source for deciding whether a trademark shall be protected or not on the ground that it would be descriptive or constitute a non-protectable geographic indication, as done in a recent case of the Swiss Federal Supreme Court²⁸⁵.

The issue (and the resulting concern) is that this increased *reliance* on technology should not be turned into an excessive *dependence* on technology. Technology should continue to serve the law and shall not control it. The hypothetical «person skilled in the art» should continue to be the legal reference under patent law and shall not be replaced by a computer or a database «skilled in the art». Similarly, Internet search engines and other massive data processing technologies shall not be viewed as the exclusive sources for assessing whether a document is part of the state of the art because of its (alleged) online availability at a given date.

Technological tools must (of course) be used in the application of the law and can be validly relied upon, provided that the role and the limits of technology are clearly understood and identified and that all the required measures are taken in order to ensure that such technologies are and remain trustworthy. This implies an intensive and transdisciplinary interaction between law (and legal people) and technology (and technology people). There cannot be any good technology-related legal solutions without deeper understanding of the techno-

285 See ATF 135 III 416 para. 2.3: «Si on utilise le moteur de recherche le plus fréquemment employé (i.e. Google), on constate que le mot «Calvi» fait apparaître en premier lieu des sites consacrés à la ville corse, et non pas à des villages italiens ou à des personnes physiques. Il faut en déduire que le terme «Calvi» évoque le plus naturellement la cité corse. Il s'agit donc d'un nom géographique qui peut en principe être interprété comme une indication de provenance»; this is however not undisputed, see LISA LARRIMORE OUELLETTE, The Google Shortcut to Trademark Law, 102 California Law Review (2014), p. 351–407, available at: <<https://www.law.stanford.edu/publications/the-google-shortcut-to-trademark-law>> (who concludes her article – p. 407 – with a «broader claim», according to which «Google results can supplant a significant portion of current trademark strength and likelihood-of-confusion inquiries»).

logy issues which are at stake. This interaction must furthermore be on-going because of the fast evolving technological environment. The law should consequently develop creative tools and mechanisms in order to ensure that it can react and adapt to this constantly changing environment. The law and the justice should thus become more dynamic. Rather than regulating and deciding in a (too) static manner that a certain conduct complies (or not) with the law at the time when the decision is made or the law adopted, the law should be conceived and justice should be rendered in a dynamic, future-oriented way²⁸⁶. Legal standards should however remain legal standards and shall not be turned into technological standards. Technology can help in applying the law but technology should not replace the law²⁸⁷. It is consequently essential that human decision processes, factors and values shall remain at the core of the legal system, while obviously acknowledging the major benefits that society as a whole can derive from the Internet and being aware that the Internet is not only a most valuable business and societal tool, but that it may also affect and even predict how humans (even lawyers) act and even think²⁸⁸. In this respect, it is comforting to note that fundamental legal principles are still viewed as offering essential guiding values, as reflected by the reference to the legal standard of reasonableness²⁸⁹ that was discussed in this report (because this standard is relevant both for the protection of trade secrets and for the issue of FRAND licensing of stan-

286 A very interesting example of this evolution is the recent decision of the Swiss Federal Supreme Court about «Google Street View» in which the Court decided that Google had to take all technological measures in order to ensure the complete anonymization of the persons and other identifying images taken by Google Street View (in order to comply with Swiss personal data protection law) and that Google also had to constantly adapt the automatic anonymization technologies to the latest state of the art (ATF 138 II 346 consid. 14.1: «Die Beschwerdeführerinnen sind verpflichtet, mit allen zur Verfügung stehenden technischen Mitteln eine vollständige Anonymisierung anzustreben und die automatische Anonymisierung laufend dem Stand der Technik anzupassen» (italics added)); this example shows that the Court expressly requested the adaptation over time of the technological measures and thus adopted a dynamic approach; on this issue (from the perspective of copyright law), see JACQUES DE WERRA, *Défis du droit d'auteur dans un monde connecté*, sic! 2014, no 4, p. 194–211 and p. 202, 209–210, available at: <<http://archive-ouverte.unige.ch/unige:36864>>.

287 This concern was famously expressed in the seminal works of Lawrence Lessig, specifically his celebrated book *Code and Other Laws of Cyberspace*, New York 2001, see the updated (wiki-based) version at: <<http://codev2.cc/>>.

288 On the impact of the Internet on the functioning of the human brain, see the thought-provoking book of NICHOLAS CARR, *The Shallows: What the Internet Is Doing to Our Brains*, W. W. Norton & Company, New York 2011.

289 Whereby this standard can apply in a variety of legal fields, see e.g. PETER GAUCH, *Der vernünftige Mensch – Ein Bild aus dem Obligationenrecht*, in: *Das Menschenbild im Recht*, Festgabe der Rechtswissenschaftlichen Fakultät zur Hundertjahrfeier der Universität Freiburg, Fribourg 1990, p. 177–203; PATRIK R. PAYER, *Das «vernünftige» Verwaltungsratsmitglied oder der objektivierte Fahrlässigkeitsbegriff in der aktienrechtlichen Verantwortlichkeit*, in: Gaudenz G. Zindel/Patrik R. Peyer/Bertrand Schott (eds), *Festgabe zum 65. Geburtstag von Peter Forstmoser*, Zurich 2008, p. 85–102; GIANNI SUPPA, *Grundlegendes Recht: Der vernünftige Mensch im Strafrecht*, Basel 2003; see also the analysis of MICHAEL SALTMAN, *The Demise of the «Reasonable Man»*, A Cross-Cultural Study of a Legal Concept, New Brunswick/London 1991 and

dard essential patents). We can thus hope and expect that these standards shall continue to apply and to guide lawmakers, courts, regulators, companies and citizens in the information age.

4. While many of the legal issues discussed in this report are global by their very nature and arise in similar terms around the world (also because they frequently result or derive from provisions of international or regional intellectual property conventions, such as the TRIPS or the EPC), the question remains of the potential role of individual countries, and specifically of Switzerland, in contributing to the discussion about these global issues. This role should not be underestimated: at a time when global Internet users are looking for safe harbors and safe places for hosting and preserving their confidential digital assets²⁹⁰, it would be adequate and even welcome if Switzerland and Swiss law were to play an active and leading role in assessing whether and how the legal framework for the protection and use of confidential information in the Internet era shall be adapted. This mission appears justified for a variety of reasons, particularly because Switzerland is privileged to host many global stakeholders which are key actors in the Internet policy debate and also because the Swiss political institutions strongly support this role²⁹¹. While the debate is and should obviously remain global, while it can and should also take place online

GEORGE P. FLETCHER, *The Right and the Reasonable*, 98 *Harvard Law Review* (1985), p. 949–981.

290 See LAURA SECORUN PALET, *Switzerland: From Banking Paradise To Data Safe Zone*, NPR, July 12, 2014, available at: <<http://www.npr.org/2014/07/12/330751548/switzerland-from-banking-paradise-to-data-safe-zone>>; ARCHANA VENKATRAMAN, *Is Switzerland turning into a cloud-haven in the wake of Prism scandal?*, *Computer Weekly*, July 5, 2013, available at: <<http://www.computerweekly.com/news/2240187513/Is-Switzerland-turning-into-a-cloud-haven-in-the-wake-of-Prism-scandal>> (it being noted that these sources emphasize the importance of Swiss data protection regulations).

291 See the parliamentary proposal (motion) ref. 14.3423 submitted by the member of the National Council Ruedi Noser on June 10, 2014 for the purpose of positioning Switzerland as an international platform for Internet governance, which was accepted by the Swiss Federal Council on September 3, 2014 and by the Swiss Parliament (by the National Council on September 26, 2014 and by the Council of States on March 3, 2015), see the website: <http://www.parlament.ch/e/suche/Pages/geschaefte.aspx?gesch_id=20143423>; in connection with this parliamentary proposal, the Federal Department of Foreign Affairs and the Swiss Office of Communications jointly launched in April 2014 the «Geneva Internet Platform», which offers an observatory, a capacity building centre (online and *in situ*), and a centre for discussion about Internet governance and policies (<<http://giplatform.org/>>), that other institutions have joined (i.e. the Geneva Centre for the Democratic Control of Armed Forces (DCAF), the ETH Board and the University of Geneva), see <<http://giplatform.org/events/official-launch-geneva-internet-platform>>; the Geneva Internet Platform is cited in a recent report of the Swiss Federal Council about the measures aiming at reinforcing the role of Switzerland as host country (for international organizations), see «Message concernant les mesures à mettre en œuvre pour renforcer le rôle de la Suisse comme Etat hôte», of November 19, 2014, *Federal Gazette* 2014, p. 9029, p. 9056 (available at: <<http://www.admin.ch/opc/fr/federal-gazette/2014/9029.pdf>>); the Foreign Affairs Committee of the Council of States has approved the report of the Swiss Federal Council at its session of April 13–14, 2015, see press release of April 14, 2015, available <<http://www.parlament.ch/e/mm/2015/Pages/mm-apk-s-2015-04-14.aspx>>.

(on a variety of virtual discussion platforms), there are legitimate reasons for conducting Internet policy discussions in Switzerland²⁹². Thinking and discussing globally about the regulation of the intangible world of Internet and of on-line networks does not – and should not – prevent local actions and initiatives in any given country.

292 See URS GASSER/JENS DROLSHAMMER, *The Brave New World of (Swiss) Law: Contours of a Framework and Call for a Strategy to Shape Law's Digital Revolution*, available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2602789>.