Chapter 4. Mapping the notion of secrecy

§ 1 Secrecy in the digital age

A) Increasing vulnerability of confidential information

The advent of new technologies in the globalised world has allowed individuals and companies to generate and share information at a much faster pace than ever before. The flow of information is unprecedented to the point that some suggest that we now live in a "data centred economy".[1267] In effect, the ever-growing amount of data available, mostly through the Internet, may be deployed to unlock new sources of economic development, foster scientific progress and scrutinise governments' actions.[1268] Despite the numerous advantages, the increase in information is creating a host of new problems. Indeed, it is becoming more and more difficult to ensure data security and personal privacy.[1269]

Legislators all around the globe are trying to adapt to the changes brought about by the widespread and constant information exchange. A prime example of this is the comprehensive reform of the Data Protection framework undertaken by the EU Commission with the adoption of the GDPR and the publication of the Final Report on the e-commerce sector inquiry led by the Commission.[1270] In the same vein, in 2012, the U.S. Federal Government announced the Big Data Research and Development Initiative, which aimed at facilitating the gathering, organisation and access to big sets of digital data.[1271] The adoption of the DTSA in the U.S. and the

---

1267 'Data, data everywhere' *The Economist* (London, 25 February 2010) <http://www.economist.com/node/15557443> accessed 15 September 2018; see further Gintare Surblyte, '6th GRUR Int / JIPLP Joint Seminar: Internet search engines in the focus of EU competition law – a closer look at the broader picture' [2015] GRUR 127, 130.

1268 'Data, data everywhere' *The Economist* (London, 25 February 2010) <http://www.economist.com/node/15557443> accessed 15 September.

1269 Ibid.

1270 Commission, 'Final report on the E-commerce Sector Inquiry' COM(2017) 229 final <http://ec.europa.eu/competition/antitrust/sector_inquiry_final_report_en.pdf> accessed 15 September 2018.

1271 'Obama Administration unveils "Big Data" Initiative: Announces $ 200 million in new R&D investments' (29 March 2012) <https://www.whitehouse.gov

TSD in the EU is set against this backdrop. The convergence of protection on both sides of the Atlantic was prompted, among other reasons, by the increasing vulnerability and strategic importance of confidential information.[1272] In effect, the Impact Assessment prepared by the Commission during the TSD legislative process identified five main factors underpinning the increasing difficulties in concealing trade secrets, which partially correspond to those mentioned by the perfume industry representatives.[1273] They are: (i) labour mobility, (ii) globalisation, (iii) longer supply chains, (iv) the information-intensive economy that we live in, and (v) the shortening of production cycles and the rise of fast-moving industries.[1274]

Without doubt, it is now easier to store large amounts of business sensitive information in a single spreadsheet document or on a computer hard drive, which can also be downloaded within seconds on to a USB thumb-drive or uploaded to the cloud and reach a broader audience much faster.[1275] Even though this clearly facilitates the effective management of information within firms, it also increases the risk of leakage of valuable information. By way of illustration, in 2006 the Texas District Court had to decide on a preliminary injunction preventing a former employee who had downloaded the equivalent of 1,5 million raw pages on to several USB thumb-drives before leaving his job and had subsequently copied the downloaded files on to his personal computer and the system of his new employer from working for any competitor.[1276] The use of servers also poses new risks for trade secret holders, as the vast amounts of data that were previously stored in physical cabinets or document warehouses are now available to hundreds of employees in a company through the mere clicking a mouse.[1277] Similar concerns apply to the general use of laptop computers, which allow employees to take valuable information outside the premises of their companies or to remotely access it from anywhere in

/sites/default/files/microsites/ostp/big_data_press_release.pdf> accessed 15 September 2018.

1272 Victoria A. Cundiff and others 2016 (n 789) 738.

1273 See chapter 5 § 4 B).

1274 Impact Assessment (n 385) 15-16.

1275 Elizabeth A. Rowe, 'Contributory Negligence, Technology, and Trade Secrets' [2009] 17 George Mason LR 1, 14.

1276 In *Anadarko Petroleum Corp. v. Davis*, 2006 WL 3837518 (S.D. Tex. Dec. 28, 2006) the court denied the preliminary injunction, but the parties entered into an Agreed Order, whereby the competitor unterook to return all proprietary information and to refrain from using such information.

1277 Elizabeth A. Rowe 2009 (n 1275) 14.

the world through virtual private networks ("VPN").[1278] This has facilitated both the physical misappropriation of information (for instance, through the theft of the laptop), as well as unauthorised access to data stored on a server or computer by hackers.[1279]

Furthermore, the advent of digital technologies has made the dissemination of valuable secret information easier; now it can be done with the "mere push of a button".[1280] Notably, this has been facilitated by the widespread use of email communications within companies that allow employees to send sensitive information from their corporate account to their personal accounts, or even to competitors, as well as instant messaging services, such as Skype and Google Hangouts. Similarly, posting confidential information on the Internet has become an increasing threat for companies, which risk losing their valuable trade secrets if an employee inadvertently or maliciously posts them on an Internet website and, as a result, the information becomes generally known.[1281]

In view of the above, it is undeniable that in the digital age it has become much harder to conceal information from competitors and the public at large. This, in turn, calls into question how secrecy should be construed vis-à-vis its frontiers with the public domain and, ultimately, enquires about the optimal scope of protection. The following section underscores the main difficulties in this regard.

B) Constructing the public domain

Defining the boundaries of the public and private spheres is of utmost importance in every legal system. In the realm of intellectual property, this is particularly challenging, as constructing and defining the contours of private rights and the intangible objects to which they refer is seemingly more complex than with regard to tangible property.[1282]

In the context of confidentiality, "the public domain" is an expression that has been used for decades to designate information that cannot be the

1278 Elizabeth A. Rowe 2009 (n 1275) 14.
1279 Elizabeth A. Rowe 2009 (n 1275) 14.
1280 Elizabeth A. Rowe 2009 (n 1275) 16.
1281 Elizabeth A. Rowe 2009 (n 1275) 16.
1282 Nari Lee, 'Public domain at the interface of trade mark and unfair competition law: The case of referential use of trade marks' 309, 309 in Nari Lee, Ansgar Ohly, Annette Kur, Guido Westkamp (eds), *Intellectual Property, Unfair Competition and Publicity* (Edward Elgar 2014).

object of trade secrets protection.[1283] More generally, it has also been deployed to refer to "material that is unprotected by Intellectual Property Rights".[1284] Indeed, the construction of the public domain has been studied extensively in connection to copyright and patents. However, in the field of trade secrets it has attracted less scholarly discussion. This mostly results from the casuistic nature of trade secrets protection, as well as from the fact that there is no universally accepted definition of the public domain. Its boundaries change from jurisdiction to jurisdiction and evolve with time.[1285] Thus, an innovation that was initially kept secret by an undertaking may be discovered by competitors through reverse engineering or independent creation and enter the realm of the public domain after some time. Similarly, it has been suggested that the abstract definition of the public domain does not necessarily correspond to the actual information that a departing employee may use in his new employment.[1286]

Despite these inherent difficulties, mapping the public domain has normative significance, as it allows for identifying the relevant values underpinning its components.[1287] To be sure, a solid public domain is necessary to foster creativity and innovation.[1288] More specifically, according to Samuelson, it allows for creating new knowledge, and encourages competition through imitation, as well as follow-on innovation. Thus, a robust public domain is essential to promote access to information in the academic, scientific and cultural spheres.[1289] In the field of trade secrets this is even more problematic, as the subject matter protected may never enter

---

1283 Charles Tait Graves 2007 (n 337) 39, footnote 145; see for instance in the US: *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 484 (1974) stating that "by definition a trade secret has not been placed in the public domain"; similarly *Storage Tech. Corp. v. Custom Hardware Eng'g & Consulting Inc.*, 421 F.3d 1307, 1319 (Fed Circ. 2005) "Information that is in the public domain cannot be appropriated by a party as its proprietary trade secret"; *VD, Inc. v. Raytheon Co.*, 769 F.2d 842 (1st Cir. 1985): "Once a trade secret enters the public domain, the possessor's exclusive rights to the secret are lost".

1284 James Boyle, 'Foreword: The Opposite of Property?' [2003] 66 Law and Contemporary Problems 1, 30.

1285 Pamela Samuelson, 'Challenges in Mapping the Public Domain' 7, 13 in P. Bernt Hugenholtz and Lucie Guibault (eds), *The Public Domain of Information* (Kluwer International Law 2006).

1286 Charles Tait Graves 2007 (n 337) 87-88.

1287 Pamela Samuelson 2006 (n 1285) 13.

1288 Nari Lee 2014 (n 1282) 311.

1289 Pamela Samuelson 2006 (n 1285) 13; for a more detailed overview of the discussion surrounding the public domain see Lawrence Lessig, *Free Culture* (The Penguin Press 2004).

the public domain. Unlike formal IPRs, trade secrets are not subject to any time limitation.[1290] Thus, the pool of information available to individuals and companies is diminished as the protection of trade secrets increases.[1291]

In the light of the above, determining whether a specific piece of information has lost its secret nature and accordingly entered the public domain is crucial to assess whether it can be used by third parties other than the original holder or the recipient of the information bound by a confidentiality obligation, or whether such an obligation remains enforceable. This is essential, for instance, in the case of departing employees who may intend to use information that they have acquired during the course of their employment relationship or for licensees that wish to cease paying their licensing fees. At the same time, as explained in chapter 1, the protection of a company's secret valuable information appears necessary and justified from a utilitarian perspective (and to a certain extent, also from a deontological one).[1292] Thus, in view of the increasing challenges in concealing digital information, it is of utmost importance to find the appropriate balance between the secret sphere and the public domain. The following sections are devoted to analysing the principles that govern such an appraisal: namely, whether something is generally known or readily accessible.

To this end, first the different concepts and requirements of trade secrets protection followed in Germany and England before the implementation of the TSD are examined (§ 2). From this comparative analysis, some interpretative principles regarding the definition of trade secrets laid down in Article 2 TSD and the subject matter protected are proposed (§ 3). Next, the dissertation goes on to examine the essential features of the notion of secrecy in greater depth, namely the degree of secrecy required (§ 4 A), the concept of readily ascertainability (§ 4 B), and the effects of the disclosure (§ 4 C) through the lenses of English, German and U.S. case law. In the light of this comparative analysis, some conclusions as to the interpretation of the relevant circles doctrine are drawn (§ 4 D). Thereafter, in § 4 E, the secrecy standard is compared to other IPRs, such as novelty in patent law and originality in copyright law, with a view to finding an equilibrium between the different legal regimes. Next, the possibility of resorting to trade secrets protection for Big Data sets is analysed under § 4F (Excursus).

1290 William van Caenegem 2014 (n 7) 13-14.
1291 William van Caenegem 2014 (n 7) 14.
1292 See chapter 1 § 2.

The ultimate goal of this investigation is to underscore the principles that courts across EU jurisdictions should follow in order to determine, in a consistent manner, whether information is part of the public domain or remains secret pursuant to Article 2(1)(a) TSD. Notwithstanding the aforementioned, such an analysis is largely factually driven. For that reason, it is only possible to outline general guiding principles.

§ 2 *Different concepts and requirements for protection of trade secrets before the implementation of the TSD*

A) Concept and requirements for the protection of trade secrets in Germany

I. Distinction between Geschäftsgeheimnis and Betriebsgeheimnissen

In Germany, unlike other jurisdictions, no statutory definition of trade secrets exists. Instead, the following working definition has been developed by the courts:

> A trade secret is information which relates to a particular business, is known only to a narrow limited number of persons, so is secret, and under the express or identifiable (as a rule, commercial) owner's will, which is based on a legitimate interest, is intended to be kept secret.[1293]

Article 17 UWG distinguishes between two categories of trade secrets, namely commercial secrets ("*Geschäftsgeheimnisse*") and industrial secrets ("*Betriebsgeheimnisse*"). The former refers to the business-related information of an undertaking,[1294] such as customers' and suppliers' data, or contractual and cost estimation documents,[1295] while the latter encompasses technical information.[1296] Among others, courts have ruled that industrial

1293 Translation by Gintare Surblyte 2011 (n 182) 49; BGH MMR 2006, 815, 816 – *Kundendatenprogramm*; BGH GRUR 2003, 356, 358 – *Präzisionsmessgeräte.*
1294 Gintare Surblyte 2011 (n 182) 49.
1295 *Ohly*/Sosnitza (n 813) § 17 Rdn 5.
1296 *Harte-Bavendamm*/Henning-Bodewig (n 376) § 17 Rdn 1.

secrets are manufacture and assembly processes,[1297] formulas[1298] or computer programs.[1299]

At first glance, the division of trade secrets into two categories might appear merely formal, as no definition of any of these concepts is provided, either in § 17 UWG or throughout the Act. Notwithstanding this, during the *travaux préparatoires* of the UWG (1896) it was extensively debated whether commercial information should be covered by the legal regime for the protection of trade secrets.[1300] Accordingly, an explicit distinction was included for the purposes of clarity, which unequivocally stated that commercial information fell within the scope of § 9 UWG 1896 (now § 17 UWG). However, in practice, no substantial legal consequences arise from such a distinction[1301] other than the exclusive application of § 18(1) UWG to industrial secrets ("*Betriebsgeheimnisse*").[1302] Thus, the terms "business secret" ("*Unternehmensgeheimnis*") and "economic secrets" ("*Wirtschaftsgeheimnis*") are often used as generic terms ("*Oberbegriff*").[1303]

II. Requirements for the protection of trade secrets

As stated in the previous section, the definition of trade secrets that has been followed by case law requires that (i) information, (ii) must be connected to a particular business, (iii) must not be public, but only known by a limited circle of people, (iv) must be kept secret by the express will of the trade secret holder, and (v) the desire to keep the information secret must be based on an economic interest.[1304]

1297 BGH GRUR 1963, 367 – *Industrieböden*.
1298 BGH GRUR 1980, 750 – *Pankreaplex*.
1299 BGH GRUR 1977, 539 – *Prozessrechner*; *Köhler*/Bornkamm/Feddersen (n 835) § 17 Rdn 12a.
1300 Björn H. Kalbfus, K*now-how Schutz in Deutschland zwischen Strafrecht und Zivilrecht-welcher Reformbedarf besteht?* (1st edn, Carl Heymanns Verlag 2011) 70.
1301 Lutz Lehmer, *UWG: Kommentar zum Wettbewerbsrecht* (Luchterhand 2007) 555; *Ohly*/Sosnitza (n 813) § 17 Rdn 5, Axel Beater (n 811) § 22 Rdn 686; *Köhler*/Bornkamm/Feddersen (n 835) § 17 Rdn 4a.
1302 Lutz Lehmer 2010 (n 1301) 555.
1303 *Ohly*/Sosnitza (n 813) 17 Rdn 5; Gintare Surblyte 2011 (n 182) 49; Björn H. Kalbfus 2011 (n 1300) 70; *Harte- Harte-Bavendamm*/Henning-Bodewig (n 376) § 17 Rdn 1; hereinafer, the generic term "trade secret" will be used.
1304 BGH GRUR 2009, 603, Rdn 13 – *Versicherungsvertreter*; Hirsch/Ann/*Brammsen*, *Münchener Kommentar zum Lauterkeitsrecht* (2nd edn, C.H. Beck 2014) § 17 Rdn 8; Florian Schweyer 2012 (n 99) 458.

The following sections analyse the requirements for the protection of information as a trade secret in the German jurisdiction.

1. Information

The working definition adopted by the German courts refers to facts ("*Tatsachen*"). The use of this term has been criticised for not being sufficiently precise, because the law of trade secrets protects information about facts ("*Tatsachen*") and not the facts themselves.[1305]

2. Information connected to a business — Geschäftsbezogenheit

In Germany, information can only be protected as a trade secret if it can be ascribed to a particular business,[1306] i.e. the information must be "used in relation to the business"[1307] or owned and controlled by the said business.[1308] No other requirements regarding the content or the object of the secret information have to be met.[1309]

Consequently, private secrets[1310] and information that stems from universities and research institutions do not fall within the scope of §§ 17 and 18 UWG.[1311] This contrasts with the broad scope of the English breach of confidence action and the broad interpretation of commercial value followed by courts in the U.S. The rationale behind such a limitation derives from the very foundations of unfair competition.[1312] The legal regime for the protection of trade secrets was established with the intention of safeguarding the "exercise without disruption of the business activity"[1313] of

1305 See Stephan Hillenbrand, *Der Begriff des Betriebs- und Geschäftsgeheimnisses* (Herbert Utz Verlag 2017) 28 and Björn H. Kalbfus 2016 (n 1122)1010 with further references.
1306 See Florian Schweyer 2012 (n 99) 458; Gintare Surblyte 2011 (n 182) 50.
1307 Rudolf Kraßer 1970 (n 831) 589; Michael Knospe (n 834) § 15:5; Gintare Surblyte 2011 (n 182) 49.
1308 Florian Schweyer 2012 (n 99) 458; Michael Knospe (n 834) 15:5.
1309 Axel Beater (n 811) Rdn 1878.
1310 *Ohly*/Sosnitza (n 813) § 17 Rdn 6.
1311 Florian Schweyer 2012 (n 99) 458 noting that in other jurisdictions, like the United States, they are actually considered trade secrets.
1312 *Harte-Bavendamm*/Henning-Bodewig (n 376) § 17 Rdn 2.
1313 *Harte-Bavendamm*/Henning-Bodewig (n 376) § 17 Rdn 2.

the trade secret holder in order to preserve the market position that he had obtained through his secret knowledge and experience.[1314]

From the outset it was controversially discussed, as happened in most jurisdictions, whether the information protected under the trade secrets legal regime should meet the patentability requirements set forth in the German Patent Act.[1315] In 1907, one of the first decisions rendered by the Supreme Court of the German Reich regarding trade secret protection, the *Pomril*[1316] judgement, ruled out such a possibility, stating that: "It is not relevant whether the (…) process was new in the sense of §§ 1,2 of the Patent Act (…)".[1317] Later on in the same decision, it was further noted that a known process could be the object of a trade secret only if by keeping the information secret the trade secret holder could achieve a certain competitive advantage.[1318] The principles set out by the *Pomril* decision have been incorporated by subsequent case law.[1319]

Likewise, courts have repeatedly stated that it is irrelevant whether the information is secret as such, or whether only its relationship with the business is kept secret. This issue was first clarified by the Supreme Court of the German Reich in the *Stiefeleisenpresse* decision.[1320] In the legal reasoning of this landmark case, the court noted that a known process could be the object of a trade secret, as long as its use by the business was not disclosed. It further added that the relationship with the company lasted for as long as the trade secret holder had a legitimate economic interest in keeping the relationship between the process and the undertaking confidential. Hence, the relationship with the company is not lost by the mere fact of selling the product in which the trade secret is embodied.[1321]

1314 *Harte-Bavendamm/*Henning-Bodewig (n 376) § 17 Rdn 2.

1315 See § 3 German Patent Act.

1316 RGZ 1907 65, 333, 335 – *Pomril*.

1317 RGZ 1907 65, 333, 335 – *Pomril* (…)"kommt es nicht darauf an, ob das Promil Verfahren in dem Sinne neu war, in dem eine Erfindung nach §§ 1, 2 des Patentsgesetz neu sein muß, wenn die patentfähig sein soll". This point of view has been reiterated in subsequent case law, for example: RGZ 1935 149, 329, 335– *Stiefeleisenpresse;* BGH GRUR 1995, 424, 426 – *Möbelpaste*.

1318 RGZ 1907 65, 333, 335 – *Pomril*; RGZ 1935 149, 329, 334 – *Stiefeleisenpresse*, BGH GRUR 1995, 424 – *Möbelpaste.*

1319 Florian Schweyer 2012 (n 99) 459.

1320 RGZ 1935 149, 329, 335 – *Stiefeleisenpresse*.

1321 *Ohly/*Sosnitza (n 813) § 17 Rdn 6.

In this context, it has been stated that the *information connected to business* requirement correlates with the condition that "information is lawfully within the control" of its holder, spelt out in Article 39(2) TRIPs.[1322]

3. Secrecy — Nichtoffenkundigkeit

By definition, the subject matter of trade secrets protection must not be in the public domain.[1323] Pursuant to the prevailing view in case law, information will be regarded as secret as long as it is neither generally known nor easily accessible.[1324] The threshold for assessing these requirements is the so-called "circle of experts" ("*Fachkreise*") but also the competitors, whose actions are ultimately the object of the UWG regulation.[1325]

Information will only be regarded as secret if it is "only known by a limited circle of people".[1326] Consequently, in Germany, the relevant yardstick has become whether the trade secret owner maintains control over the number and type of persons who know or who have access to the information.[1327] Thus, courts do not resort to a precise numerical value in order to evaluate if the "number of persons who have knowledge of the information is sufficiently limited".[1328] Instead, a case-by-case analysis is con-

---

1322 *Ohly*/Sosnitza (n 813) § 17 Rdn 6.

1323 Michael Knospe (n 834) 15:8.

1324 Florian Schweyer 2012 (n 99) 459, Michael Knospe (n 834) 15:8; *Ohly*/Sosnitza (n 813) § 17 Rdn 7; *Harte-Bavendamm*/Henning-Bodewig (n 376) § 17 Rdn 3.

1325 Florian Schweyer 2012 (n 99) 461; Thomas Reimann,'Einige Überlegungen zur Offenkundigkeit im Rahmen von §§ 17 ff. UWG und von § 3 PatG' [1998] GRUR 298, 299; BGH GRUR 2012, 1048 Rdn 21 – *Movicol (Zulassungsantrag)*: "Das BerGer. hat zutreffend angenommen, dass es nicht zu einer den Geheimnischarakter ausschließenden allgemeinen Bekanntheit führt, wenn die Zulassungsunterlagen einem begrenzten – wenn auch unter Umständen größeren – Personenkreis zugänglich waren, etwa den auf Grund des Arbeitsvertrags zur Verschwiegenheit verpflichteten Betriebsangehörigen oder auch bestimmten Kunden und Lieferanten. Nichts anderes gilt, soweit die Unterlagen den mit der Vorbereitung und Prüfung des Zulassungsantrags dienstlich befassten Personen bekannt geworden sind"; this topic is further elaborated in chapter 4 § 4 D) III.

1326 *Ohly*/Sosnitza (n 813) § 17 Rdn 8.

1327 *Ohly*/Sosnitza (n 813) § 17 Rdn 8; Rudolf Kraßer, 'Grundlagen des zivilrechtlichen Schutz von Geschäfts- und Betriebsgeheimnissen sowie von Know-how' [1977] GRUR 177, 178.

1328 Michael Knospe (n 834) 15:4.

ducted,[1329] where the decisive factor is the likelihood of a disclosure to any third parties, in particular competitors, not bound by a confidentiality obligation.[1330] Hence, courts have deemed that the trade secret holder is in control of the secret, not only among his employees, who are bound by their labour contracts, but also with regard to licensees and contract manufacturers, so long as they are expressly bound by a confidentiality obligation.[1331]

As stated above, information will be deemed public and thus not protectable under trade secrets law, not only if it is generally known, but also if it may be easily accessed ("*leichte Zugänglichkeit*").[1332] This requirement comprises both actual access and the possibility of accessing the information concerned.[1333] In patent law, a disclosure that is theoretically accessible by any third party is considered novelty destroying pursuant to § 2 of the German Patent Act,[1334] whereas under the trade secrets regime, the accessibility requirement has been construed in a much narrower and "specific" sense.[1335] Information that can only be obtained in an extremely difficult manner is considered to meet such a condition and consequently can be protected as a trade secret.[1336] This highlights one of the defining features of trade secrets vis-á-vis other IPRs: in order to be protected information must fulfil neither the technical novelty criterion as applied in patent law, nor the originality requirement necessary to grant copyright law.[1337]

In the light of the above, a new standard for the assessment of secrecy was developed by case law, according to which "information which in its specific manifestation can only be obtained through great difficulty and cost ("*große Schwierigkeit und Opfer*") is considered to be secret".[1338] In contrast, information that can be learned by the interested parties without such difficulty is deemed to be dedicated to the public and thus part of the public domain. The development of this standard was considered neces-

1329 *Ohly*/Sosnitza (n 813) § 17 Rdn 8.
1330 *Harte-Bavendamm*/Henning-Bodewig (n 376) § 17 Rdn 4; Rudolf Kraßer 1977 (n 1327) 177.
1331 Rudolf Kraßer 1977 (n 1327) 179.
1332 Florian Schweyer 2012 (n 99) 461.
1333 Rudolf Kraßer 1977 (n 1327) 179; Florian Schweyer 2012 (n 99) 462.
1334 See § 2 German Patent Act.
1335 Henning Harte-Bavendamm 2010 (n 823) § 77 Rdn 11.
1336 Rudolf Kraßer 1977 (n 1327) 179; Thomas Reimann 1998 (1325) 298, 299.
1337 Hirsch/Ann/*Brammsen* (n 1304) § 17 Rdn 13; BGH GRUR 1995, 424, 426 – *Möbelpaste.*
1338 Rudolf Kraßer 1977 (n 1327) 179.

sary in order to protect competitors who acquired a secret independently and through a high investment of effort and costs.[1339] Thus, information does not necessarily lose its secret nature if third parties achieve similar results independently.[1340]

4. Will to keep the information secret — Geheimhaltunsgswille

The fourth requirement applied by courts sets forth that information must remain undisclosed as a result of the will of the trade secret holder.[1341] The rationale behind this subjective requisite[1342] is to differentiate mere unknown information from information that is intentionally kept secret.[1343] The will to observe confidentiality must stem from the holder and it can be agreed upon orally or in a written form,[1344] even though it will often be inferred from the circumstances of the case.[1345] Courts have construed the intent requirement in a broad sense, encompassing both the "potential" and the actual intent.[1346] In addition, it has been suggested that if such intent is unclear, employees should presume that "all knowledge and processes, whose existence is unknown outside the inner sphere of the particular business and that play a role in its competitive position",[1347] are kept undisclosed as a result of the express will of the trade secret holder.[1348] Thus, the burden of proof lies with the employee, who will have to provide evidence that the employer did not intend to keep the information undisclosed.[1349] Likewise, actual knowledge of the secret information by the employer is not required, so long as if he had in fact been acquainted

1339 Rudolf Kraßer 1977 (n 1327) 179; Henning Harte-Bavendamm 2010 (n 823) § 77 Rdn 10.
1340 Henning Harte-Bavendamm 2010 (n 823) § 77 Rdn 10.
1341 BGH GRUR 1964, 31 – *Petromax II.*
1342 Gintare Surblyte 2011 (n 182) 51.
1343 *Ohly*/Sosnitza (n 813) § 17 Rdn 11; Henning Harte-Bavendamm 2010 (n 823) § 77 Rdn 12.
1344 Henning Harte-Bavendamm 2010 (n 823) § 77 Rdn 12.
1345 Henning Harte-Bavendamm 2010 (n 823) § 77 Rdn 12.
1346 Axel Beater (n 811) § 22 Rdn 1880.
1347 Henning Harte-Bavendamm 2010 (n 823) § 77 Rdn 12; BGH GRUR 2006, 1044 Rdn 19 – *Kundendatenprogramm.*
1348 Henning Harte-Bavendamm 2010 (n 823) § 77 Rdn 12.
1349 Henning Harte-Bavendamm 2010 (n 823) § 77 Rdn 12; Florian Schweyer 2012 (n 99) 468, Michael Knospe (n 834) 15:4.

with it he would have intended to keep it secret.[1350] This general presumption refers to the situation where information was developed by employees but still had to be communicated to employers, and it was introduced for practical purposes, because there is always a period of time between the actual invention and the act of communication.

This requirement has been strongly criticised by several commentators, who believe that the way in which it is tailored nowadays renders it a superfluous condition for protection.[1351] Some argue that establishing such a fiction appears redundant and should be abandoned.[1352] Hence, the only relevant yardstick should be whether the trade secret holder had disclosed the information and consequently it had become generally known.[1353]

5. Interest in keeping the information secret — Geheimhaltungsinteresse

The will to keep information secret ("*Geheimhaltungswille*") is closely connected with the last requirement set forth by case law for protecting trade secrets, namely the interest in keeping the information undisclosed ("*Geheimhaltungsinteresse*").[1354] Nowadays, it is generally accepted by case law and academia that the trade secret holder must have a justifiable economic interest in keeping the information secret, as the mere intention is deemed an inadequate subjective parameter for assessing trade secrets protection.[1355] Such an objective condition was essentially introduced with the aim of ensuring that the owner could not arbitrarily establish the information covered by the trade secret, irrespective of whether an objective un-

1350 Florian Schweyer 2012 (n 99) 468; BGH GRUR 1977, 539 – *Prozessrechner*.

1351 In that sense, Henning Harte-Bavendamm 2010 (n 823) § Rdn 12 states that "Die Erkannbarkeit dieses Willens mag für die Strafbarkeit wegen Geheimnisverrat von Bedeutung sein, jedoch nicht für den Begriff des Geheimnisses und nicht unbedingt für zivilrechtliches Vorgehen".

1352 *Ohly*/Sosnitza (n 813) § 17 Rdn 11.

1353 *Ohly*/Sosnitza (n 813) § 17 Rdn 11.

1354 Rudolf Kraßer 1970 (n 831) 590.

1355 In this sense, BGH GRUR 1955, 424, 425– *Möbelwachspaste*: "Der Begriff des Betriebsgeheimnisses außer dem Willen zur Geheimhaltung ein berechtigtes wirtschaftliches Interesse des Betriebsinhabers an der Geheimhaltung voraussetze"; *Ohly*/Sosnitza (n 813) § 17 Rn 12; *Köhler*/Bornkamm/Feddersen (n 835) § 17 Rdn 9; Henning Harte-Bavendamm 2010 (n 823) § 77 noting that "Außer dem Willen zur Geheimhaltung ist ein berechtigtes wirtschaftliches Interesse des Betriebsinhabers an der Geheimhaltung erforderlich".

derlying justification existed.[1356] In that regard, it should be noted that §§ 17 and 18 of the UWG are criminal law provisions and accordingly set forth criminal penalties in the event of infringement.[1357]

The ground for the assessment of the so-called "justifiable interest" is based on the competitive advantage gained by keeping the specific information secret, in line with Article 39(2)(b) TRIPs. Hence, case law has introduced a general presumption, whereby a legitimate economic interest will be assumed if the disclosure of the information hinders the rightholder's position in the market, or conversely, it leads to an improvement in the competitor's position.[1358] However, this does not mean that the trade secret must have economic value as such.[1359] Likewise, as already stated with regard to the secrecy requirement, it is not necessary that the object of protection is undisclosed information from a company, such as a secret method of manufacture. It suffices that its relationship with the business is kept secret. For instance, based on the previous example, the method for manufacture could be generally known, but if its use by a given company remains secret this relationship could constitute the object of trade secrets protection.[1360]

As a final consideration, it should be pointed out that it is irrelevant whether the protected secret deals with immoral or unlawful information.[1361] Notwithstanding this, a disclosure might be justified on the basis of third parties' best interests and, arguably, an obligation to do so may arise in the event of an emergency situation pursuant to § 34 of the Criminal Code.[1362]

1356 Henning Harte-Bavendamm 2010 (n 823) 13; *Ohly*/Sosnitza (n 813) § 17 Rdn 12.
1357 Gintare Surblyte 2011 (n 182) 47.
1358 *Köhler*/Bornkamm/Feddersen (n 835) § 17 Rdn 9.
1359 *Köhler*/Bornkamm/Feddersen (n 835) § 17 Rdn 9.
1360 *Köhler*/Bornkamm/Feddersen (n 835) § 17 Rdn 9.
1361 Henning Harte-Bavendamm 2010 (n 823) § 77 Rn 13; *Köhler*/Bornkamm/Feddersen (n 835) § 17 Rdn 9; Stephan Hillenbrand, *Der Begriff des Betriebs- und Geschäftsgeheimnisses* (Herbert Utz Verlag 2017) 75.
1362 Henning Harte-Bavendamm 2010 (n 823) § 77 Rdn 13; *Köhler*/Bornkamm/Feddersen (n 835) § 17 Rdn 9.

B) The notion of confidentiality in England

I. Concepts of confidential information and trade secret in England

The inclusion of trade secrets within the general legal framework created by the breach of confidence action has led to the establishment of a very complex system, where the boundaries between privacy and secrecy have progressively faded, causing the concepts to merge. In numerous rulings, English courts have sought to provide a uniform interpretation of essential concepts, such as confidential information, trade secrets and know-how.[1363] The following paragraphs attempt to shed light on the complex and at times confusing terminology used in case law when applying the breach of confidence action.

Confidential information is most adequately defined as the general term used to refer to information that is protected under the breach of confidence action.[1364] As mentioned previously, its scope covers all types of information without restrictions on the subject matter of protection,[1365] irrespective of the format in which it is presented.[1366]

As regards *trade secrets*, no statutory definition of this term has been enacted into law in England.[1367] A detailed study of the authorities on the subject reveals that the English courts have mostly avoided precisely delineating the semantic contours of this concept.[1368] As such, trade secrets refer to one of the several categories of information that are protected under the

1363 The difficulties of establishing a uniform interpretation of confidential information were already outlined by Lord Megarry in *Thomas Marshall (Exports) Limited v Guinle* [1979] FSR 208 (Ch), 209 where he held that "it is far from easy to state in general terms what is confidential information or trade secret".

1364 John Hull, 'Trade Secret Licensing: the art of the possible' [2009] 14 JIPLP 203, 205.

1365 Tanya Aplin and others 2012 (n 22) para 6.02 state that confidential information can be generally classified in four kinds, i.e. trade secrets, artistic and literary information, government secrets and personal information. However, it is further noted that "the boundaries separating these categories are not always easy to draw and there is a certain amount of overlapping".

1366 Lionel Bently and Brad Sherman 2014 (n 125) 1144.

1367 Notwithstanding, the Freedom of Information Act 2000, s 43(1) refers to trade secrets.

1368 John Hull 2013 (n 934) 158.

breach of confidence action,[1369] although some commentators argue that the courts have applied this phrase such that is has a two-fold meaning.[1370]

The first and more restrictive approach limits the scope of trade secrets to post-employment restraints on former employees, based both on express and implied duties of confidentiality.[1371] This was the case in *Helmet Integrated Systems Ltd v Tunnard*, where Moses J noted that former employees should be free to use and apply for their own benefit the skill and knowledge acquired and developed during the course of an employment relationship, even if it entails competing with the former employer. However, he added that they should not benefit from information regarded as a trade secret.[1372]

Conversely, the prevailing and broader approach uses the term trade secrets as a "synonym for commercial and industrial confidential information",[1373] similarly to Article 2(1) TSD. Indeed, Megarry J in *Thomas Marshall (Exports) Limited v Guinle* stated that trade secrets are information concerning industrial and trade settings that meets the following four requirements:

(i) First, the disclosure of the information would be detrimental to its holder or to the benefit of a competitor or any other third party;
(ii) Second, the owner should believe that the information concerned is secret;
(iii) Third, the holder's belief under the two previous requirements "must be reasonable";
(iv) Fourth, information must be assessed according to the "usage and practices of the particular industry or trade concerned".[1374]

Against this background, the traditional distinction between technical secrets and business secrets is also applicable. In particular, *know-how* is con-

1369 John Hull 2013 (n 934) 161.
1370 Tanya Aplin and others 2012 (n 22) para 6.06.
1371 See among others *Faccenda Chicken Ltd v Fowler* [1987] Ch 117 (CA), 136 where *Neil LJ* highlighted that: "The implied term which imposes an obligation on the employee as to his conduct after the termination of the employment is more restricted in scope than that which imposes a general duty of good faith. It is clear that the obligation not to use or disclose information may cover secret processes of manufacture such as chemical formulae (…), or designs or special methods of construction (…), and other information which is of sufficiently degree of confidentiality as to amount to a trade secret".
1372 *Helmet Integrated Systems Ltd v Tunnard* [2007] FSR 385 (CA), 445-446.
1373 Tanya Aplin and others 2012 (n 22) para 6.06.
1374 *Thomas Marshall (Exports) Limited v Guinle* [1979] FSR 208 (Ch), 229.

sidered to encompass two kinds of technical information.[1375] On the one hand, it is used to refer to non-patented practical information that has been developed through experience and testing and that is secret, substantial and identified.[1376] On the other hand, know-how has been used to designate the set of skills and knowledge that employees acquire during the course of their employment. This was the view supported, among others, by Sir Thomas Bingham M.R. in *Lancashire Fire Ltd v Lyons*, where it was held that:

> The normal presumption is that information which the employee has obtained in the ordinary course of his employment, without specific steps such as memorising particular documents, is information which he is free to take away and use in alternative employment.[1377]

With the above clarification in mind, the following section delves into two of the four conditions that are necessary to find liability under the breach of confidence action mentioned above: (i) the subject matter capable of protection, and (ii) the confidential nature of the information.[1378]

II. Subject matter capable of protection

One of the most notable features of the English legal system is the fact that the breach of confidence action places no restrictions on the type of information protected and the format in which it is conveyed.[1379] Accordingly, the action has been invoked to protect both oral and written information,[1380] as well as drawings,[1381] photographs[1382] and products.[1383] Notwithstanding this, courts have developed four limitations as to the information that falls under its scope of protection. Consequently, trivial information, information that is vague, immoral information and false infor-

1375 Tanya Aplin and others 2012 (n 22) para 6.10; John Hull 2009 (n 1364) 206.
1376 Similar to Article 1(i) TTBER.
1377 *Lancashire Fires Limited v S.A. Lyons & Company Limited and Others* [1996] FSR 629 (CA), 656.
1378 See chapter 3 § 3 C) II.
1379 Lionel Bently and Brad Sherman 2014 (n 125) 1144.
1380 *Fraser v Thames Television Ltd* [1984] QB 44 (QB).
1381 *Morison v Moat* [1851] 9 Hare 241.
1382 *Douglas v Hello! Ltd and others* [2007] UKHL 21.
1383 *Vestergaard Frandsen A/S v Bestnet Europe Ltd* [2013] UKSC 31; *Helmet Integrated Systems Ltd v Tunnard* [2007] FSR 16 (CA).

mation are not eligible for protection.[1384] Each of these exceptions will be analysed in turn.

1. Commercial value: protection of trivial information?

As a first general limitation, case law has provided that trivial information may not be subject to a confidential obligation. Famously, Megarry J in *Coco v A.N.Clark (Engineers) Ltd* stated that "equity ought not to be invoked merely to protect *trivial tittle-tattle*, however confidential".[1385] Yet, the decision provided no further guidance on how to assess such a requirement. The Oxford dictionary defines *tittle-tattle* as referring to "casual conversation about other people, typically involving details that are not confirmed as true; gossip".[1386] In line with this definition, in *Attorney General v Guardian Newspapers Ltd* Lord Goff stressed "the duty of confidence applies neither to useless information, nor to trivia".[1387] However, in *Stephens v Avery*[1388] the notion that information concerning an extramarital affair between two people published in a tabloid was not eligible for protection under the breach of confidence action was rejected. In this case, the plaintiff, Mrs Stephens, conveyed in confidence certain information of a private nature to one of the defendants, Mrs Avery. In particular, the information related to a lesbian relationship between the plaintiff and Mrs Telling, who because of the affair was murdered by her husband. Subsequently, Mrs Avery communicated the information about the lesbian relationship to one of the most prominent tabloids in the UK, "The Mail on Sunday", in which an article revealing details of the relationship was published in July 1984. As a result, Mrs Stephens brought an action for a breach of confidence. Upon Appeal, Sir Nicolas noted that the exclusion of "trivial tittle-tattle" information in *Coco v A.N.Clark (Engineers) Ltd* was exclusively concerned with information that was of industrial value and expressed scepti-

1384 Lionel Bently and Brad Sherman 2014 (n 125) 1144.
1385 *Coco v A.N.Clark (Engineers) Ltd* [1969] RPC 41 (Ch), 48; later Judge Dean in *Moorgate Tobacco Co, Ltd v Philip Morris Ltd* (No 2) [1984] 156 CLR 414, 438.
1386 'tittle-tattle, n' (*OED Online*, OUP June 2013) <https://en.oxforddictionaries.com/definition/tittle-tattle> accessed 15 September 2018.
1387 Lord Goff in *Attorney General v Guardian Newspapers Ltd (No. 2)* [1990] 1 AC 109 (HL), 282.
1388 *Stephens v Avery* [1988] FSR 510 (Ch).

cism about considering the sexual conduct of an individual as trivial tittle-tattle information.[1389]

Accordingly, courts have been wary of regarding information as trivial, partially due to the uncertainty and difficulty related to the consideration of what constitutes trivial information,[1390] which in practice has led to a reduction in the applicability of this limitation.[1391]

Notwithstanding this, in the field of trade secrets, some decisions have demanded information to be commercially valuable or at least attractive, in line with Article 2(1)(b) TSD.[1392] Yet, a survey of the cases involving trade secrets protection reveals that most of them do not expressly refer to the value of the information, as it is often deemed that companies would not bring legal action if the information concerned did not have a certain "value".[1393]

More recently, the notion of "objective value" was used as one of the factors that signalled whether the information possessed the necessary quality of confidence.[1394] In addition, in the landmark decision from the House of Lords *Douglas v Hello and other Ltd* the fact that the parties entered into an agreement covering the protection of information was considered crucial in assessing the confidential nature of the pictures of the wedding that had been misappropriated.[1395] In view of this, it appears that "commercial value" as such is not a normative requirement under the breach of confidence

---

1389 *Stephens v Avery* [1988] FSR 510 (Ch), 515.

1390 Lionel Bently and Brad Sherman 2014 (n 125) 1000.

1391 Lionel Bently and Brad Sherman 2014 (n 125) 1001.

1392 For instance, in *Thomas Marshall (Exports) Limited v Guinle* [1979] FSR 208 (Ch), 229 it was stated that one of the requirements to find liability was that the disclosure of the information should cause a prejudice to the owner or an advantage to competitors or third parties; see further Lionel Bently and Brad Sherman 2014 (n 125) 1000; Gintare Surblyte 2011 (n 182) 78.

1393 Tanya Aplin and others 2012 (n 22) para 5.51; however, in *Nichrothermc Electrical Co Ltd v Percy* [1956] RPC 272 (Ch) the plaintiffs brought legal action for the misappropriation of a machine that presented no commercial value.

1394 *HEFCE v Information Commissioner and the Guardian News and Media Ltd* (EA/2009/0036, 10 January 2010) [48].

1395 See *Douglas v Hello! Ltd and others* [2007] UKHL 21 [325] (Lord Brown): "Having paid £1m for an exclusive right it seems to me that OK! ought to be in a position to protect that right and to look to the law for redress were a third party intentionally to destroy it. Like Lord Hoffmann, I would uphold OK!'s claim, as Lindsay J did at first instance, on the ground of breach of confidence"; however Lord Walker [299] held the opposite view, by noting that "the confidentiality of any information must depend on its nature, not on its market value".

action in England, but it is a strong indicator of the existence of information that is worth protecting.[1396]

2. Information that is vague

In addition to being non-trivial, the general principle is that confidential information should be specific i.e. clear and identifiable.[1397] Vague or general information is excluded from the scope of the breach of confidence action.[1398] In effect, as noted in *Terrapin Ltd v Builders' Supply Co (Hayes) Ltd.* by Roxburh J, confidential information must be "something that can be traced to a particular source and not something which has become so completely merged in the mind of the person informed that it is impossible to say from what precise quarter he derived the information which led to the knowledge which he is found to possess".[1399]

Identifying the information for which protection is sought is crucial not only to establish the duration of an injunction and the amount of damages due, but also to elucidate whether an actual breach has occurred.[1400] It also appears of paramount importance in the context of the licensing agreements in order to delineate the scope of the contracts.[1401]

Such a limitation has often been invoked by courts as a ground to deny granting an injunction preventing the use of a "generalized body of information".[1402] Consequently, injunctions should be drafted in a very specific manner so as to allow defendants to know with certainty which conducts are permitted and which are forbidden. This is particularly relevant, for instance, in injunctions relating to post employment restraints as regards trade secrets.[1403] In the event of litigation, the trade secrets that former employees are not allowed to use after the termination of their employment relationship should be clearly identifiable in any potential injunction. It is

---

1396 Nevertheless, Roger M. Toulson and Charles M. Phipps 2012 (n 326) 3-081 suggest that "There must be some value to the party claiming confidentiality (not necessarily commercial) in the information being treated as confidential".
1397 Roger M. Toulson and Charles M. Phipps 2012 (n 326) para 3-086.
1398 Lionel Bently and Brad Sherman 2014 (n 125) 1001-1003.
1399 *Terrapin Ltd v Builders' Supply Co (Hayes) Ltd* [1962] RPC 375 (Ch), 391; a detaied account of this case is provided in chapter 6 § 2 B) III. 3).
1400 Tanya Aplin and others (n 22) para 5.74.
1401 John Hull 2009 (n 1364) 208.
1402 Tanya Aplin and others (n 22) para 5.74.
1403 Roger M. Toulson and Charles M. Phipps 2012 (n 326) para 3-088.

essential to distinguish them from general skills and knowledge, which every employee should be free to use.[1404] The importance of identifying the information that constitutes the trade secret in order to find liability under the breach of confidence action was restated by the Supreme Court in *Vestergaard v Bestnet*, a case concerning an alleged breach by a former employee.[1405]

The above should not be understood to mean that simple ideas cannot be protected, even though the more novel or original ideas are, the more likely they are to merit protection.[1406] As opposed to copyright law, the breach of confidence action affords protection to ideas without the need to show their specific expression.[1407] By way of illustration, the ideas for a new TV programme[1408] and an innovative concept of a dance club were deemed confidential.[1409] Yet again, the courts have struggled to draw a line with regard to when an idea is sufficiently detailed. Notably, this requirement has been construed as meaning that the concept or idea must be "sufficiently developed to be capable of being realized".[1410] This is analysed further in the assessment of the secrecy requirement vis-à-vis IPRs normative standards.[1411]

1404 *Faccenda Chicken Ltd v Fowler* [1987] Ch 117 (CA), 122-123.

1405 *Vestergaard Frandsen A/S v Bestnet Europe Ltd* [2013] UKSC 31, [22]: "It would seem surprising if Mrs Sig could be liable for breaching Vestergaard's rights of confidence through the misuse of its trade secrets, given that she did not know (i) the identity of those secrets, and (ii) that they were being, or had been, used, let alone misused. The absence of such knowledge would appear to preclude liability, at least without the existence of special facts".

1406 See Tanya Aplin and others 2012 (n 22) para 5.55.

1407 William Cornish, David Llewellyn and Tanya Aplin 2013 (n 209) para 8-10 note that "an idea for something to be elaborated may attract legal protection as confidential information where there is nothing that generates copyright".

1408 *Fraser v Thames Television Ltd* [1984] QB 44 (QB).

1409 *De Maudsley v Palumbo* [1996] FSR 447 (Ch).

1410 Lionel Bently and Brad Sherman 2014 (n 125) 1145-1146 noting that this is criterion was first developed in the Supreme Court of Victoria in *Tablot v General Television Corp* [1981] RPC 1.

1411 Chapter 4 § 4 E) II 2).

3. Immoral and false information

In England the general principle is that immoral information is not eligible for protection under the breach of confidence action.[1412] However, as no generally accepted code of morality exists, courts have shown reluctance to apply this limitation. For instance, in *Stephens v Avery*, while the court ruled that in abstract a duty of confidence would not be enforceable against "matters which have a grossly immoral tendency", it concluded that no common view existed on the immoral nature of sexual relationships between consenting adults.[1413]

Another unsettled issue is whether false information (i.e. inaccurate information) can be protected under the breach of confidence action, particularly due to its intersection with the defamation cause of action.[1414] A review of leading academic works on confidentiality seems to support that inaccuracies should not affect the confidential nature of the information, provided that such an action is not intended to cover a defamation claim,[1415] as noted by the Court of Appeal in *McKennitt v Ash*.[1416] This case concerned the publication of a book on the life of the plaintiff, a Canadian folk singer. In the book, private information about the singer was disclosed by the author, a former friend and business partner. As regards the falsity of the allegations, the court concluded that, "the truth or falsity of the information is an irrelevant inquiry in deciding whether the information is entitled to be protected".[1417] However, some commentators have noted that these arguments seem less persuasive with regard to non-private or non-personal matters, such as government information.[1418] Indeed, in *Financial Times Ltd & Ors v Interbrew SA* the leakage of five documents that contained false information about the acquisition of a brewery in South Africa was not deemed enforceable under the breach of confidence action, because in the words of Sedley J, "there can be no confidentiality in false information".[1419] In sum, it appears that case law under the breach of con-

1412 William Cornish, David Llewellyn and Tanya Aplin 2013 (n 209) paras 8-10.
1413 *Stephens v Avery* [1988] FSR 510 (Ch).
1414 Roger M. Toulson and Charles M. Phipps 2012 (n 326) para 3-093.
1415 Tanya Aplin and others (n 22) para 5.67; Roger M. Toulson and Charles M. Phipps 2012 (n 326) para 3-093; *McKennitt v Ash* [2006] EWCA Civ 1714 (CA).
1416 *McKennitt v Ash* [2006] EWCA Civ 1714 (CA), [86].
1417 *McKennitt v Ash* [2006] EWCA Civ 1714 (CA), [86].
1418 Tanya Aplin and others (n 22) para 5.62 and para 5.72.
1419 *Financial Times Ltd. & Ors v Interbrew SA* [2002] EWCA Civ 274 (CA), [27]-[28].

fidence action provides no clear answer as to the protection of false information.

III. Confidential nature of the information

Crucially, in order to bring an action under an alleged breach of confidence, it must always be proved that the disclosed information is of a confidential nature i.e. "it possesses the necessary quality of confidence". Despite the widespread use of this term, few English cases seem to provide a satisfactory definition.[1420]

In assessing this requirement, courts tend to follow a pragmatic approach, where the analysis of confidentiality is considered against the specific background of every particular case.[1421]

The following sections examine the general test developed by English courts, along with the main attributes of confidentiality.

1. The general test of inaccessibility

The tests developed to assess confidentiality are mostly of an objective nature, as they do not take into account the views of the parties.[1422] Indeed the "status of the information is a question of fact, not intention".[1423] Notwithstanding this, Toulson and Phipps have propounded that an implicit principle is that courts should only recognise confidentiality in those cases where it appears *reasonable* to do so.[1424] This is argued on the basis that a number of cases have resorted to the "reasonable man yardstick" when assessing the confidential nature of the information (and not just whether an obligation of confidence arises),[1425] and the fact that secrecy is

1420 John Hull 1998 (1016) para 3.03.
1421 Tanya Aplin and others 2012 (n 22) 149.
1422 Allison Coleman 1992 (n 911) 8; this was also noted in *Lancashire Fires Limited v S.A. Lyons & Company Limited and Others* [1996] FSR 629 (CA), 656: "the subjective view of the owner cannot be decisive. There must be something which is not objectively a trade secret, but something which was known, or ought to have been known, by both parties to be so".
1423 Lionel Bently and Brad Sherman 2014 (n 125) 1148.
1424 Roger M. Toulson and Charles M. Phipps 2012 (n 326) para 3-082.
1425 *Thomas Marshall (Exports) Limited v Guinle* [1979] FSR 208 (Ch), 229 and chapter 3 § 3 C) II. 2. a).

often defined by its limits, in which "reasonableness" is often invoked.[1426] Yet, this view is not supported because it introduces an element of subjectivity, ("the owner's belief -which must be reasonable- that the information is confidential") that should only be taken into account in the assessment of whether an obligation on the recipient arises, not as regards the status of the information.[1427]

In effect, most decisions follow the objective test of confidentiality first developed in *Saltman Engineering v Campbell Engineering*, where confidentiality was defined by the limitations imposed by the public domain:

> The information, to be confidential, must, I apprehend, apart from contract, have the necessary quality of confidence about it, namely it must not be something which is public property and public knowledge. On the other hand, it is perfectly possible to have a confidential document, be it a formula, a plan, a sketch, or something of that kind, which is the result of work by the maker upon materials which may be available for the use of anybody; but what makes it confidential is the fact that the maker of the document has used his brain and thus produced a result which can only be produced by somebody who goes through the same process.[1428]

As is apparent from the above passage, for information to qualify as confidential it should meet two requirements. The first is rather broad and demands that information is not "public property" or "public knowledge", i.e. part of the "public domain".[1429] Secondly, Lord Griffin suggested a test, according to which information would only be deemed confidential if it could only be acquired through the reproduction of the mental process that led to the creation of the resulting information.

In the light of the above, courts have applied the general principle of "inaccessibility" with the aim of assessing whether certain information falls into the public domain.[1430] This judgement is based on a confidentiality test developed by subsequent authorities, according to which information

---

1426 Roger M. Toulson and Charles M. Phipps 2012 (n 326) 3-082 and footnote 142 for an account of the cases in which "reasonableness" is invoked.

1427 John Hull 1998 (1016) para 3.09.

1428 *Saltman Engineering v Campell Engineering* [1948] 65 RPC 203 (CA), 215.

1429 Law Commission 1981 (n 327) 27 noting that "in referring to this requirement the courts have used a variety of expressions, but it has become increasingly common to say that the information for which protection is sought by the action of breach of confidence must not be in the public domain".

1430 Tanya Aplin and others 2012 (n 22) paras 5.14 -5.39.

will only be deemed confidential if "special intellectual skill and labour" are essential in order to reproduce it.[1431] That is understood to mean that the alleged infringer would have to go through the same burdensome mental process as the confider.[1432] This criterion is applied to information considered in its entirety, irrespective of its components.[1433]

Against this background, it is noteworthy that generally known information can also be deemed confidential, so long as intellectual skill and labour are required in order to compile it.[1434] This rationale has been applied to decide on cases concerning the confidential nature of customer lists, where the data on individual customers were also available in other trade databases. However, the lists in their entirety were regarded as confidential, as competitors had to undergo the same intellectual labour as the creators of the lists.[1435]

Drawing on the foregoing, it appears that courts in England have adopted a "relative secrecy" approach, as opposed to patent law, where the standard for assessing the novelty of an invention is an absolute one. Information can be conveyed to a limited number of people without losing its confidential nature.[1436] The issue lies in determining the extent of publication permitted. The general principle is that once information is generally accessible and widespread it cannot be regarded as confidential.[1437] Similarly,

---

1431 Tanya Aplin and others 2012 (n 22) para 5.15; *Ocular Sciences Ltd v Aspect Vision Care Ltd* [1997] RPC 289 (Ch), 375.

1432 Tanya Aplin and others 2012 (n 22) 5.16.

1433 *Coco v A.N.Clark (Engineers) Ltd* [1969] RPC 41 (Ch), 47.

1434 Tanya Aplin and others 2012 (n 22) para 5.17.

1435 *International Scientific Communications Inc v Pattinson and Others* [1979] FSR 429 (Ch), 434.

1436 Lionel Bently and Brad Sherman 2014 (n 125) 1148 ; *Franchi v Franchi* [1967] RPC 149 (Ch), 152: "Clearly a claim that the disclosure of some information would be a breach of confidence is not to be defeated simply by providing that there are other people in the world who know the facts in question besides the man as to whom it is said that his disclosure would be a breach of confidence and those to whom he had disclosed them. It must be a question of degree depending on the particular case, but if relative secrecy remains, the plaintiff can still succeed".

1437 See *Attorney General v Guardian Newspapers Ltd (No 2)* [1990] 1 AC 109 (HL), 282 where Lord Goff stated that: "In particular, once it has entered what is usually called the public domain (which means no more than that the information in question is so generally accessible that, in all the circumstances it cannot be regarded as confidential) then, as a general rule, the principle of confidentiality can have no application to it".

the fact that information can be obtained from reverse engineering should not deprive the information of its secret nature.[1438]

In this context, it should be indicated that "the status of information may change over time" and that information that is in the public domain may become secret if the public forgets the information or the relevant public changes.[1439]

In the light of the above, it is clear that establishing whether information is confidential is a question of fact that should be assessed on a case-by-case basis.[1440] Against this background, Hull refers to an Australian case in which a multi-factor test to assist in determining whether a specific piece of information presented the "necessary quality of confidence" was developed. The factors taken into consideration were:

(i) The extent to which the information was known outside the plaintiff s business;
(ii) The extent to which the information was known to employees and others inside the plaintiff's business;
(iii) The extent to which the plaintiff had taken measures to safeguard the information;
(iv) The value of the information to the plaintiff' competitors;
(v) The amount of effort expended by the plaintiff in developing the information; and
(vi) The ease or difficulty with which the information could properly be acquired.[1441]

While these factors are to be weighed against each other, the assessment of secrecy is ultimately factually driven. No normative value can be attached to either of them. In particular, the adoption of measures (factor 3), the value of the information (factor 4) and the cost of development (factor 5) signal the existence of information worth protecting, which may nevertheless be generally known.

In sum, it appears that the English notion of confidentiality is very similar to the concept of "*Nichtoffenkundigkeit*" followed under German law. In both jurisdictions, the crucial test to assess secrecy consists of looking into whether the information can only be obtained through great difficulty and

---

Paul Lavery,'Secrecy, Springboards and the Public Domain' [1998] 20 EIPR 93, 95.

1438 John Hull 1998 (1016) para 3.18.
1439 Lionel Bently and Brad Sherman 2014 (n 125) 1153.
1440 John Hull 1998 (1016) para 3.06.
1441 John Hull 1998 (1016) para 3.07 citing the Austalian case *Section Pty v DelawoodPty Ltd* [1991] 21 IPR 136.

cost ("*große Schwierigkeit und Opfer*" in Germany), which is just another way of referring to the "intellectual skill and labour" yardstick propounded in the English jurisdiction under the test of inaccessibility. However, a cardinal distinction between the two jurisdictions is that English cases seem to emphasise the need to prove that intellectual skill (not just labour) is necessary to obtain the information. In addition, English case law does not refer to the fact that information loses its secret nature when it is known among the "circle of experts" that usually deal with the information in question.[1442] The reason behind this distinction can be traced back to the fact that the scope of the breach of confidence action is not confined to the protection of trade secrets, but also covers artistic and literary information, private information and government information. However, a review of the case law concerning trade secrets reveals that decisions referring to trade secrets define the public domain by reference to a narrow field, industry or profession, similar to the "relevant circle yardstick" followed under German law.[1443]

2. Form of the information

In England courts have also been confronted with the issue of deciding whether the disclosure of information in a specific form leads to its disclosure in another form. This particular topic was discussed by the House of Lords in the famous *Douglas v Hello!* case, which concerned the unauthorised publication of pictures of the wedding of the actors Michael Douglas and Katherine Zeta-Jones by Hello! magazine.[1444] The pictures published by Hello! were taken without permission by an undercover photographer who had then sold them to the defendant. As a result, both the couple and OK! Magazine brought legal action against Hello! under the breach of confidence action. Crucially, some months before the event, the couple had reached an exclusive licensing agreement with OK! Magazine, granting this publication the exclusive right to publish pictures of the event in exchange for consideration. The salient issue in this case was to decide whether protection under the breach of confidence could extend to pho-

1442 Paul Lavery,'Secrecy, Springboards and the Public Domain' [1998] 20 EIPR 93, 93 suggests that this has been required in some cases in Ireland and Australia to find a breach of confidence.

1443 John Hull 1998 (1016) para 3.16.

1444 *Douglas v Hello! Ltd and others* [2007] UKHL 21.

tographs that were already in the public domain, as the pictures had been published by national newspapers some hours before OK! Magazine came out. In rendering the decision, Lord Hoffman concluded that the object of confidentiality was "any picture of the wedding", as this was the only possible way of protecting the interests of OK!.[1445]

3. No need to adopt reasonable measures

One remarkable difference between the English breach of confidence regime prior to the implementation of the TSD and the legal system laid down in Article 39(2) TRIPs (but also in the U.S. under the UTSA and the DTSA)[1446] is that protection is not subject to the adoption of reasonable steps by the trade secret holder to safeguard the secret nature of the information. While the adoption of such measures is assessed in a positive manner by the English courts, legal commentators seem to agree on the fact that it is not a precondition for meriting protection.[1447] Notwithstanding this, in *Thomas Marshall (Exports) Limited v Guinle* the adoption of reasonable measures was considered as one of the four requirements for the protection of trade secrets.[1448]

§ 3 *The concept of trade secret in the Directive: considerations in the light of the comparative analysis*

A) Preliminary remarks

The subject matter covered by the TSD is set out in Article 1(1), which "lays down rules on the protection against the unlawful acquisition, disclosure and use of trade secrets". Thereupon, Article 2(1) provides a definition of trade secrets, which is identical to the one set forth in Article 39(2) TRIPs. In order to be protected, trade secrets must (a) be information that

---

1445 *Douglas v Hello! Ltd and others* [2007] UKHL 21 [123]; similar considerations were applied in *Creations Records Ltd v News Group Newspaper Ltd* [1997] EWHC Ch 370 (Ch), [29] which concerned the publication by tabloids in the UK of pictures of the shooting of the cover of a rock band's forthcoming album.

1446 See § 1(4) UTSA and supra chapter 4.

1447 Lionel Bently 2012 (n 114) para 3.18.

1448 *Thomas Marshall (Exports) Limited v Guinle* [1979] FSR 208 (Ch), 229.

is not generally known or readily accessible; (b) must have commercial value due to their secret nature; and (c) must be subject to reasonable steps under the circumstances to preserve secrecy. In this regard, it is worth noting that the 28 Member States of the EU are also part of the WTO and, as such, they were bound to implement the TRIPs minimum standards of protection for IPRs in their national regimes by 1 January 1996.[1449] [1450] Thus, the inclusion in the Directive of the same definition as the one provided in the TRIPs Agreement for "undisclosed information", as a minimum standard of protection, appears to be a restatement of such an obligation and provides flexibility to Member States in its implementation.[1451]

To be sure, the object of protection of Article 2(1) TSD is information, which coincides with the subject matter protected under the breach of confidence action in England and §§ 17-19 of the German UWG.[1452] Accordingly, information is deemed secret "if 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". However, upon closer examination, some uncertainty arises in connection with the meaning of some of

1449 TRIPs transitional provisions are essentially regulated in Article 65 of the Agreement. The general rule is set forth in paragraph 1, which established an automatic transitional period of one year for all WTO Members (until 1 January 1996). However, paragraphs (2) and (3) granted a four-year transitional period (until 1 January 2000) for developing countries and countries that were in the process of transformation from a centrally planned economy into a free market economy. The computing of the time referred to in Article 65 is a definite term based on the date of entry into force of the WTO Agreement. Hence, countries acceding after 1995 could not benefit from any additional transitional periods and were requested to amend their legislation before their accession, unless they qualified to benefit from the transitional periods of paragraphs (2) and (3), but only until January 1, 2000.

1450 Likewise, the European Union, as a supranational entity, became a party to the TRIPs Agreement by virtue of the Council, 'Council Decision 94/800/EC of 22 December 1994 concerning the conclusion on behalf of the European Community as regards matters within its competence, of the agreements reached in the Uruguay Round multilateral negotiations (1986-1994)' [1994] OJ L336; this is also clarified in Recital 5 TSD.

1451 In Baker McKenzie 2013 (n 1057) 5 it is noted that despite the existence of a common denominator (based on the criteria of Article 39(2) TRIPs) the definitions adopted in the different jurisdictions present divergences and in addition require particular constitutive elements.

1452 But see chapter 4 § 2 A) II. 1.

the terms used by the EU legislature and the subject matter of protection, as analysed in the following sections.

B) Terminology

The terminology used in the Directive to refer to the term trade secret and the types of information that fall under its scope are not consistently applied. Recital 14 highlights the importance of establishing a common definition without limiting the subject matter protected against misappropriation, which should cover the protection of "know-how, business information and technological information" if two conditions are fulfilled, namely, (i) there is a legitimate interest in maintaining the confidentiality of the information, and (ii) there is also a legitimate expectation in the preservation of such confidentiality. The distinction between business and technological information mirrors the practice in most Member States before the implementation of the Directive, where case law and even some statutes differentiated between industrial secrets and commercial secrets, and presents no interpretative questions.[1453]

However, the reference to know-how is confusing. It is used in the title of the Directive and in the first sentence of Recital 1 as a full synonym of trade secret, whereas Recitals 2 and 14 instead refer to it as one of the categories of undisclosed information. This is particularly problematic, as know-how is autonomously defined in Article 1(i) TTBER in a manner that seems to partially overlap with what is usually understood by "technical trade secrets" or "technological information", as mentioned in Recital 14. The use of such confusing terminology reflects the current practice in many national jurisdictions, like Germany, where know-how is regarded as an economic term rather than a legal one.[1454] Hence, for the sake of legal certainty, it would have been best if the Directive had abandoned the use of "know-how" or clarified its relationship with Article 1(i) of the TTBER.[1455]

English courts under the breach of confidence action have also used the term "know-how" to designate the set of skills and knowledge that em-

1453 As discussed in chapter 4 with regard to Germany and England.
1454 Hannes Beyerbach, *Die geheime Unternehmensinformation* (Mohr Siebeck 2012) 103; *Ohly*/Sosnitza (n 813) § 17 Rdn 11.
1455 Tanya Aplin 2014 (n 384) 264.

ployees acquire during the course of their employment.[1456] However, such an acceptation is not supported by the TSD, which provides in Recital 14 that "the definition of trade secret excludes trivial information and the *experience and skills* gained by employees in the normal course of their employment" (emphasis added).[1457] The establishment of common ground on the information that departing employees are free to use after the termination of their employment contract represents considerable progress, as Member States' practice differed substantially on this particular aspect. Notwithstanding this, the Directive provides little guidance on how to assess the boundaries between information that is actually part of a trade secret and information that constitutes "experience and skills" that employees are free to use. The TSD resorts to a vague clause that provides great flexibility to national competent courts to conduct a balancing exercise, taking into account all of the circumstances of the specific case. Some have criticised that such a broad clause will lead to an abuse of litigation,[1458] although the Directive already provides a comprehensive array of safeguards against such practices in Articles 6 to 9.

From a legislative technique perspective, the exclusion of "experience and skills gained by employees in the normal course of their employment" from the subject matter protected by trade secrets law is more problematic. This approach creates a two-tier definition of trade secret and seems unsystematically placed within the Directive. Indeed, such an assessment should be carried out in the context of the relevant liability conducts[1459] and in particular, within the balancing exercised imposed by Article 5 TSD and not at the definition level. We will return to the provisions of the TSD that regulate post-employment obligations in chapter 6, where a number of criteria to differentiate between protected trade secrets and the skill and knowledge that employees are free to use are suggested.[1460]

1456 See chapter 4 § 2 B) I.

1457 See further Article 1(3)(b) TSD.

1458 IP Federation, 'The EU Trade Secrets Directive' (2014) Policy Paper PP04/15, 3-4 <https://www.ipfederation.com/news/ip-federation-comments-on-the-compromise-text-for-the-eu-trade-secrets-directive/> 15 September 2018.

1459 Tanya Aplin 2014 (n 384).

1460 This issue is discussed in greater detail in chapter 6 § 1 A) and has recently been the object of a comprehensive study by Magdalena Kolasa, *Trade Secrets and Employee Mobility* (CUP 2018).

C) Commercial value

The second limb of the definition provides that information must have commercial value "because it is secret". In this regard, it is worth noting that before the implementation of the Directive, such a requirement was not foreseen either under the English breach of confidence action, or under German law. However, as indicated above, English cases dealing with trade secrets have viewed commercial value as a strong indicator that the information is worth protecting.[1461] In the same vein, the German "*Geheimhaltungsinteresse*" requirement has been interpreted as meaning that the trade secret holder has a commercial interest in keeping the information secret. Yet, in the latter jurisdiction such a requirement has also been invoked to protect secret information that does not confer commercial value, but the disclosure of which would be detrimental to a company (for instance, information that would harm the reputation of the company, or information about collusive practices that would result in antitrust sanctions).[1462] In addition, in Germany, a causality link between the concealed nature of the information and its value is not required.[1463]

Another question that was intensely discussed during the negotiation of the Directive was whether potential value suffices or actual value is required. The UTSA expressly mentions both, while TRIPs is silent on this point. Recital 14 TSD sheds light on this issue by stating that the value can be either actual or potential. As discussed previously,[1464] this is particularly relevant in the context of ensuring that R&D companies will have a Laboratory Zone in which to develop their ideas and innovations. The same recital provides further guidance on how to interpret the commercial value benchmark:

> Furthermore, such know-how or information should have a commercial value, whether actual or potential. Such know-how or information should be considered to have a commercial value, for example, where its unlawful acquisition, use or disclosure is likely to harm the interests of the person lawfully controlling it, in that it undermines that person's scientific and technical potential, business or financial interests, strategic positions or ability to compete. (…)[1465]

1461 Chapter 4 § 2 B) II. 1.
1462 Björn H. Kalbfus 2016 (n 1122)1011.
1463 Thomas Hören and Reiner Münker 2018(b) (n 1119) 151
1464 Chapter 1 § 2 B) IV.
1465 Recital 14 TSD.

As is apparent from the above, and in line with the principles that inform the Directive, commercial value is to be interpreted in a broad and flexible manner. It refers not only to the loss of competitive advantage, but also more generally to any harm to the scientific and technical capacity and the economic interest of the trade secret holder and his position in the market that may result from the disclosure of information. Consequently, it is submitted that protection shall also be afforded to organisations that act with no profit motive, such as universities and research institutions. This was particularly not the case under German law, where information had to be ascribed to a particular business ("*Geschäftsbezogenheit*").

Similarly, illicit activities, such as collusive practices or information that may hamper the reputation of a company, which were protected in Germany under the *Geheimhaltungsinteresse* prong, seem to be excluded from the scope of protection of the Directive by virtue of the whistle-blower exception laid down in Article 5(b) TSD, provided that the trade secret holder intended to protect "the public interest". Accordingly, it is submitted that national legislatures and judicial authorities should interpret that the notion of "trade secret" does not include information that the trade secret holder wishes to keep secret, but that does not affect his competitive position.

As a final note, Recital 14 also expressly excludes trivial information from the subject matter that can be protected as a trade secret. The adjective trivial is deemed to refer to things "of little value or importance"[1466] and resembles the exclusion of "trivial tittle-tattle" information under the breach of confidence action. However, drawing from the English experience, its application seems of limited relevance, as courts have struggled to draw a line between valuable and trivial information, and this will become increasingly difficult in the Digital Economy, where individual data may become valuable as a result of its inclusion in Big Data sets.[1467]

In sum, an analysis of the relevant provisions of the TSD that frame the commercial value requirement reveals that:

(i) There must be a causal link between the value of the information and its concealed nature;
(ii) The relevant factor is that the disclosure of the information hampers the ability to compete of the trade secret holder, which should be interpreted in a wide sense;

1466 'trivial, adj' (*OED Online*, OUP June 2013) <https://en.oxforddictionaries.com/definition/trivial> accessed 15 September 2018.

1467 As discussed in the Excursus in chapter 4 § 4 F) II.

(iii) Consequently, information developed by entities that do not have a profit making intention (such as universities or basic research centres) may also fall under the scope of protection of the Directive;
(iv) Illicit activities and information that may hamper the reputation of a company are not included within the scope of protection of the TSD, because they do not affect the competitive position of the trade secret holder.

D) Private and personal information

As regards the subject matter of protection, the Directive does not clarify whether secret private information that at the same time has commercial value is part of the subject matter that falls under the notion of a trade secret. This would typically be the case for celebrities who commercialise certain aspects of their private lives, such as in the *Douglas v Hello!* decision examined above.[1468] This factual scenario is covered by the breach of confidence action, but would not be protected in Germany as a trade secret because information would not meet the *Geschäftsbezogenheit* (information ascribed to a business) requirement. More generally, while it is true that in such cases the holders of secret information may have a *business* interest in commercialising unknown aspects of their lives,[1469] it is doubtful whether the EU has the competence to harmonise privacy law in such a broad manner.[1470]

More problematic is the relationship between the TSD and the GDPR. Recital 2 TSD expressly mentions "information on customers and suppliers" as one of the types of business information protected under the law of trade secrets. In turn, such information may fall under the category of personal data defined in Article 4(1) GDPR, which includes "information relating to an identified or identifiable natural person". In this regard, Recital 35 TSD clarifies that the TSD should not affect the rights and obligations laid down in the Data Protection Directive (which has been replaced by the GDPR). Hence, while it is doubtful that commercialising unknown information about someone's private life may qualify as a trade secret, it is clear that personal information may be protected as one according to Recital 35. For instance, the names and contact details included in a

1468 *Douglas v Hello! Ltd and others* [2007] UKHL 21.
1469 Tanya Aplin 2014 (n 384) 263.
1470 Ansgar Ohly 2013 (n 13) 40.

customer list, may be protected as a trade secret provided that they (i) are not generally known or readily accessible, (ii) present commercial value and (iii) are subject to reasonable measures under the circumstances to maintain them secret. In such a case, the trade secret holder shall nevertheless comply with the obligations set out in the GDPR. However, as outlined above, a systematic review of the relevant provisions of the GDPR and the TSD reveals that tension may arise between the interests of the trade secret holder in keeping information under his control undisclosed and the right of the data subject in accessing his personal data.[1471] Likewise, the distinction between private information which a priori seems excluded from the scope of the TSD and personal information which may be eligible for trade secret protection is not always a straightforward one, as for instance, the CJEU has regarded that information about professional activities or income falls within the scope of private information.[1472]

In the light of the above, it is submitted that further clarification in the TSD regarding its interplay with privacy law and personal data law would have been welcome.[1473] In this respect, it is concluded that the commercialisation of private information should not fall under the scope of trade secrets protection as harmonised by the Directive, because it does not affect the possibility of competition of any sort between the parties. As regards potential conflicts between the data subject and the trade secret holder, it is argued that as a matter of principle the access rights of data holders should prevail and, only where a clear, identifiable and substantial prejudice to the trade secret holder exists, a limitation on access rights is justified. However, in practice such a scenario seems unlikely, as personal data mostly become valuable trade secrets after their inclusion in larger data sets. Consequently, the disclosure of individual data to the data subject would theoretically not affect the value of the data because this does not imply a disclosure to competitors and, in any event, the relative value of individual data is rather low.

1471 Chapter 3 § 5 C) II. 1.

1472 As analysed by Juliane Kokott and Christoph Sobotta, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR' [2013] 3 IDPL 222-228; CJEU, Joined Cases C–92/09 and C–93/09 *Volker und Markus Schecke and Eifert* [2010] ECR I-11063, para 59.

1473 Tanya Aplin 2014 (n 384) 263.

E) Adoption of reasonable steps

The TSD sets out that in order to qualify for protection, the trade secret holder must adopt "reasonable steps under the circumstances (…) to keep it secret", in line with the UTSA, the DTSA and the TRIPs Agreement. Consequently, the adoption of measures has become a necessary requirement for protection.[1474] Yet, the comparative analysis conducted above[1475] reveals that such a condition has not been demanded by courts either in England or in Germany. Notwithstanding this, in the former jurisdiction it has been positively assessed as a strong indicator that the information is of a confidential nature. Similarly, in Germany, case law notes that the trade secret holder must have the will to keep it secret ("*Geheimhaltungwillen*"). The threshold of this subjective requirement has been interpreted as rather low, as courts mostly understand that an explicit manifestation is not necessary, and it suffices that the will to keep the information secret can be inferred from "the nature of the secret information".[1476]

Under the harmonised legal framework, by virtue of Article 2(1)(c) of the TSD, the adoption of measures (or steps) by the trade secret holder has become a necessary condition to enforce valuable secret information against any act of misappropriation.

However, this has not been without criticism. As outlined in the context of the U.S. jurisdiction, a number of commentators have warned of the consequences of including the third prong within the definition of trade secrets and the difficulties in assessing the "reasonableness" of the steps adopted".[1477] In this respect, it has been noted that if national courts apply such a requirement in a very strict manner, an overinvestment in physical measures spurring an arms race among competitors may take place.[1478] After all, trade secrets protection is afforded to information because of its undisclosed nature and, therefore, it is assumed that the holders of information adopt ex ante appropriate steps to preserve it. The MPI Comments echoed these concerns and highlighted that the term "step" should be interpreted as covering both physical and legal measures, such as express legal agreements. However, this cannot be construed as demanding that explicit confidentiality agreements are concluded individually with each per-

1474 Thomas Hören and Reiner Münker 2018(b) (n1119) 151-152.
1475 Chapter 4 § 2 A) and B).
1476 Björn H. Kalbfus 2016 (n 1122)1011 with further references.
1477 Chapter 2 § 2 B) II. 3. b).
1478 Chapter 2 § 2 B) II. 3.

son that comes under an obligation of confidence.[1479] In particular, courts should consider whether an implicit obligation exists by virtue of the relationship between the parties (for instance, employer-employee).

One aspect that is often overlooked is that including such a requirement as a normative condition for protection demands not only that the original trade secret holder, but also any potential third parties to whom the information is conveyed under an obligation of confidence (such as R&D partners or licensees), take proactive steps to safeguard the secrecy of the information in a continuous manner. Crucially, the adoption of such measures in the digital world usually involves contracting very costly IT surveillance services, which have to be updated on a regular basis to keep track of the more recent state of the art developments.[1480]

In the light of the above, it is submitted that to avoid wasteful overinvestment in protective measures:

(i) It cannot be expected that the holder of information and the third parties to whom it is conveyed (such as licensors or R&D partners) adopt all possible measures. Indeed, in the enforcement, courts should be mindful that the obligation concerns the means, not the outcome;

(ii) The reasonableness of the steps adopted to protect secrecy will depend on the specific circumstances of each individual case, but courts will have to take into consideration the nature of the threat of disclosure, the value of the trade secret and the cost of the potential security mechanisms. Consequently, the more valuable the information for which protection is sought is, the more sophisticated and costly the measures adopted should be;

(iii) The adoption of measures includes both physical and legal measures. In the absence of an express agreement, courts should take into consideration whether an implied duty of confidence existed by virtue of the relationship between the parties (for instance, between the employee and the employer).

F) A requirement of identification of the information concerned?

As a final note, it should be stressed that the EU legislature has not included within the definition or elsewhere in the TSD the requirement that in order to be protected information must be distinguishable from other

1479 Annette Kur, Reto Hilty and Roland Knaak 2014 (n 383) paras 19-20.
1480 Thomas Hören and Reiner Münker 2018(b) (n1119) para 15.

available information.[1481] Indeed, such a condition is expressly mentioned in the definition of know-how provided in Article 1(i)(iii) TTBER, where it is indicated that know-how for the purposes of licensing agreements must be "(iii) identified, that is to say, described in a sufficiently comprehensive manner so as to make it possible to verify that it fulfils the criteria of secrecy and substantiality". At first glance, such a condition may seem obvious, but in practice it has given rise to substantial litigation in England and the U.S.[1482] Upon closer examination, the identification of the information for which protection is sought is relevant to determine the substantive cause of action and the scope of the claim, and also in the context of licensing agreements. More importantly, it is essential to avoid abusive litigation.[1483] Consequently, it is submitted that in the enforcement of trade secrets, national courts should always demand that the plaintiff identify in a clear and precise manner the information concerned, even if it is not positively codified into law.

§ 4 Deconstructing secrecy

A) Evaluating the degree of secrecy required

The comparative law analysis conducted in the previous sections,[1484] together with the examination of the main principles that govern the protection of trade secrets under the U.S. and TRIPs legal framework (chapter 2) reveal that the standard of secrecy in all of the jurisdictions studied is a relative one. In effect, absolute (or perfect) secrecy would only occur if the holder of information did not share it with any third party. Such an approach goes against the interests of the holder in exploiting his commercial and technical secrets. The law of trade secrets developed in parallel with industrial expansion, and as such, responds to the modern needs of manufacturing processes, among which collaborative work and partnerships play a central role.[1485] Consequently, it is generally accepted that the revelation of confidential secrets to employees and other parties bound by

1481 Tanya Aplin and others 2012 (n 22) para 5.73.
1482 Charles Tait Graves and Brian D. Range, 'Identification of Trade Secret Claims in Litigation: Solutions for a Ubiquitous Dispute' [2006] 5 New JTechnology IP 68, 72.
1483 Tanya Aplin and others 2012 (n 22) para 5.75.
1484 Chapter 4 § 2.
1485 James Pooley 2002 (n 66) § 4.04[2] 25-26.

confidentiality agreements will not deprive them of their secret nature.[1486] To name some, this includes licensees, contractors, members of a joint venture and R&D partners.[1487] Otherwise, the holder's ability to profit economically from his secret would be substantially hindered. Thus, it appears that the rule of thumb is that secret information can be disclosed to those for whom knowing the information is essential and who are aware of its confidential nature.[1488]

At this point, it should be recalled[1489] that the relative secrecy yardstick has also been incorporated into patent law. Pursuant to Article 55(1)(a)EPC, information disclosed in confidence is not regarded as available on the relevant date for the purposes of assessing novelty.[1490] Furthermore, if the secrecy obligation is breached, a six-month limitation period to file for a patent is granted, after which the disclosure will be novelty destroying.[1491]

The upshot of the relative secrecy approach is that several competitors can develop the same information independently, without it theoretically becoming generally known. Yet, with time, the number of market participants within a given industry that are able to come up with that information may increase, thus eroding the trade secret and the commercial advantage that it provides, which may eventually become generally known and enter the public domain.[1492]

1486 James Pooley 2002 (n 66) § 4.04[2] 4-26; see further *In re Matter of Innovative Construction Systems, Inc.*, 793 F.2d 875, 883 (7th Cir. 1986) where it is argued that the proprietor of the information should not necessarily be the only one who knows the secret. Its knowledge by employees who were informed or should have known from the circumstances that the information in question was confidential does not render it publicly known; see also *A.L. Labs., Inc. v. Philips Roxane, Inc.*, 803 F.2d 378, 381 (8th Cir. 1986) noting that "the fact that information or data is developed in cooperation with other companies or joint ventures, or through a consultant or other party assisting in its development, does not mean that such information or data is not a trade secret. It may still be a confidential trade secret, provided that, in fact, it is known only to the ventures or consultants and is not generally known in the industry"; see also *Kewanee Oil Co.v. Bicron Corp.*, 416 U.S. 470, 475 (1974).

1487 Björn H. Kalbfus 2011 (n 1300) 70.

1488 James Pooley 2002 (n 66)§ 4.04[2] 26; *Köhler*/Bornkamm/Feddersen (n 835) § 17 Rdn 7a; Ingo Westerman, *Handbuch Know-how-Schutz* (C.H. Beck 2007) Kapitel 1, para 33.

1489 See chapter 1 § 3 A) I. 1.

1490 Lionel Bently 2012 (n 114) para 3.64.

1491 See G 3/98 [2001] OJ EPO 62.

1492 Roger M. Milgrim 2014 (n 160) § 1.07[2].

B) The doctrine of ready ascertainability and the principle of inaccessibility

I. Absence of a normative standard

One of the consequences of adopting a relative standard for secrecy is that information loses its secret nature somewhere between absolute secrecy and general knowledge, in line with Article 2(1)(a) TSD and 39(2)(a) TRIPs, which distinguishes between information "generally known or readily accessible". In turn, such a standard draws from the definition enshrined in the UTSA, where secret information is defined as "not being generally known (…) and not being readily ascertainable through proper means". The TSD and TRIPs refer to the term "accessibility", instead of "ascertainability", which underscores the factual nature that governs the appraisal of the secret nature of information.[1493] In addition, neither the Directive nor the TRIPs Agreement mention that the possibility of accessing information has to be carried out "by proper means". However, this is implied by the definition of unlawful acquisition provided for in Article 4(2)(b) TSD, which outlaws any unauthorised acquisition that is contrary to "honest commercial practices".

The secrecy-public domain scale is a broad one. At one end, "impenetrable secrets", namely those that cannot be devised even after a process of reverse engineering, remain concealed and confer great competitive advantage on their holders. At the other, information that is generally known draws the boundaries of the public domain.

However, in between, information that can only be obtained after a process of reverse engineering may signal the existence of an interest worthy of protection.[1494] The difficulty lies in defining when such information is accessible (or ascertainable)[1495] with so little or no effort so that it no

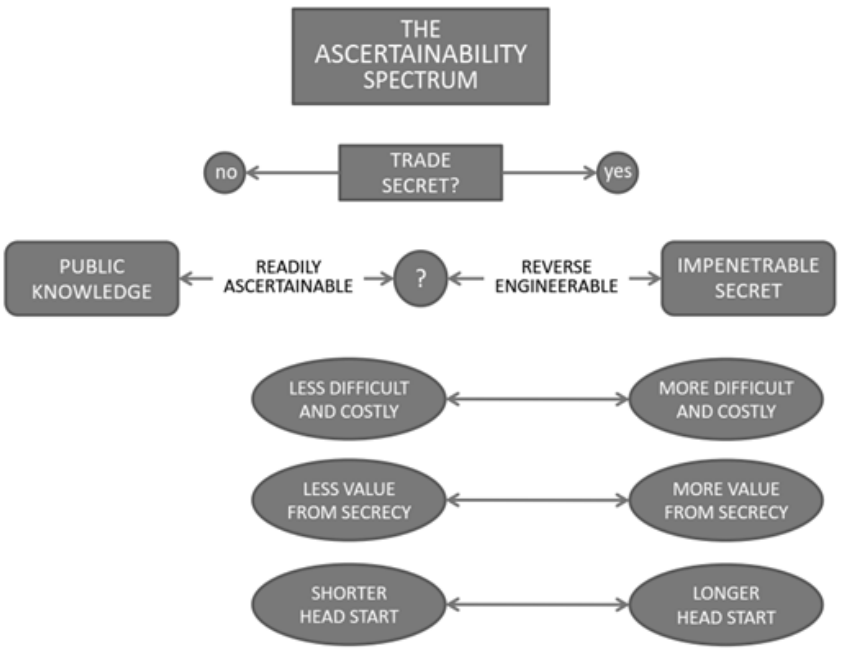
---

1493 The term 'accesible, adj' is defined in the Oxford English Dictionary as "able to be easily obtained or used" and "easily understood or appreciated", (*OED Online*, OUP June 2013) <https://en.oxforddictionaries.com/definition/accessible> accessed 15 September 2018; while 'ascertainble, adj' is defined by reference to ascertain as "find (something) out for certain; make sure of" <https://en.oxforddictionaries.com/definition/ascertain> (*OED Online*, OUP June 2013) accessed 15 September 2018 .

1494 James Pooley 2002 (n 66) § 4.04 4-41.

1495 Ascertainibility is the concept used in the UTSA, whereas Article 39(2)(a) TRIPs refers to accessibility; Nuno Pires de Carvalho 2008 (n 529) para 39.109 considers both terms to be synonyms.

longer merits protection. This is known as the "ready accessibility area" and refers to the obtention of information as such, not just the physical support in which it is embodied.[1496] However, establishing whether information is readily accessible is a complex matter and neither TRIPs nor the TSD provide guidance regarding such an assessment.[1497] Pooley attempts to shed further light on this question through a graph that depicts the accessibility (ascertainability) spectrum:[1498]



1496 Daniel Gervais 2012 (n 505) para 2.486.

1497 Gintare Surblyte, 'Enhancing TRIPS: Trade Secrets and Reverse Engineering' 725, 738 in Hanns Ullrich and others (eds), *TRIPS plus 20 – From Trade Rules to Market Principles* (Springer 2016) noting that according to the UTSA "information is readily ascertainable if it is available in trade journals, reference books, or published materials. Often, the nature of a product lends itself to being readily copied as soon as it is available on the market"; see further chapter 2 § 2 B) II. 1.

1498 Reproduced from James Pooley 2002 (n 66)§ 4.04[4] 4-42.

From the above, it can be appreciated that information that is publicly known or readily accessible does not merit protection.[1499] Thus, as the difficulty, time, labour and investment in accessing information increases, it becomes eligible for trade secrets protection. These factors signal that reverse engineering is a precondition to access information. From such a turning point onwards, the increasing difficulty further reveals that the information's economic value derived from its secrecy is higher and, in turn, the lead time advantage it confers on its holder is also longer.[1500] Such an appraisal is not merely of a theoretical nature; it is crucial to establish the duration of the injunctions in the event of misappropriation and the amount of damages. Yet again, defining the boundaries of when information is readily accessible and when it needs to undergo a process of reverse engineering is not a simple one. Nevertheless, in practice such a distinction is central. On the one hand, information that can only be obtained through reverse engineering will be protectable as a trade secret prior to undertaking such a process, whereas readily ascertainable information is part of the pool of information that any individual or company is free to use.[1501]

With the above structure in mind, it seems that the assessment of when information is readily accessible takes into account the investment (cost, time, effort, skill and labour) devoted to that end. In effect, in Germany, the prevailing standard is that of the time and effort invested in accessing the information ("*großen Zeit- oder Kostenaufwand*").[1502] In England, some cases state that information should only be regarded as confidential if it can only be acquired through the reproduction of the mental process that

1499 *Attorney General v Guardian Newspapers Ltd (No 2)* [1990] 1 AC 109 (HL), 282 stressing "the first limiting principle (which is rather an expression of the scope of the duty) is… that the principle of confidentiality only applies to information to the extent that it is confidential. In particular, once it has entered what is usually called the public domain (which means no more than that the information in question is so generally accessible that, in all circumstances, it cannot be regarded as confidential) hen, as a general rule, the principle of confidentiality can have no application to it".

1500 James Pooley 2002 (n 66)§ 4.04[4]4-42.

1501 James Pooley 2002 (n 66)§ 4.04[4]4-42.

1502 BGH GRUR, 2012, 1048 Rdn 21– *Movicol* (*Zulassungsantrag)*; *Ohly*/Sosnitza (n 813) § 17 Rdn 9; Henning Harte-Bavendamm, 'Wettbewerbsrechtliche Aspekte des Reverse Engineering von Computerprogrammen' [1990] GRUR 657, 660: "Nicht geheim ist, was von jedem Interessenten ohne größere Schwierigkeiten und Opfer in Erfahrung gebracht werden kann".

led to the creation of the resulting information,[1503] that is, if the information is the "product of the skill of the human brain".[1504]

Thus, when information can be acquired by third parties with an interest without incurring great labour, skill or cost, it is regarded as readily accessible and is automatically part of the public domain. Conversely, secrecy is preserved if interested third parties cannot acquire the information without such an investment.[1505] The test suggested by English authorities appears particularly pertinent: if information can only be obtained through the investment of intellectual skill it should be regarded as secret. Such a benchmark would in turn indicate that the obtention of information is subject to a process of reverse engineering through trial and error and consequently it merits protection. However, ultimately, such an appraisal is a matter of fact and degree, as it is not possible to find a normative standard that is applicable in all cases and allows to quantify secrecy.[1506]

Indeed, this reasoning has been questioned for its rather circular nature: information is deprived of its concealed nature when it is so generally accessible that it cannot be deemed secret neither in its parts nor in its entirety. However, its significance lies in the flexible nature of the assessment. In each individual case, courts have to consider whether the level of accessibility is such that in all conceivable circumstances a party bound by an alleged duty of confidentiality could not be required to fulfil such an obligation.[1507]

II. Criticism

The inclusion of the "ready ascertainability" benchmark within the definition of secrecy has been questioned by several commentators. In particular Risch suggests that such a factor should have been included as a defence available in the event that the competitor had actually "readily ascertained

1503 *Saltman Engineering v Campell Engineering* [1948] 65 RPC 203 (CA), 215.
1504 *Ocular Sciences Ltd v Aspect Vision Care Ltd* [1997] RPC 289 (Ch), 375.
1505 BGH GRUR 1963, 367, 370 – *Industrieböden*; Rudolf Kraßer 1977 (n 1327) 179; see also conclusion of the Law Commission 1981 (n 327) 137 "Information should not be treated as being in the public domain where it is only accessible to the public after a significant contribution of labour, skill or money has been made".
1506 Lionel Bently and Brad Sherman 2014 (n 125) 530.
1507 Roger M. Toulson and Charles M. Phipps 2012 (n 326) para 3-109-3-111.

the information through independent means".[1508] He argues that the alleged misappropriator should always provide evidence that he in fact obtained the information from a different source, in line with the California Trade Secrets Law, where the "ready ascertainability" of the information is not included within the definition of a trade secret.[1509] Risch illustrates this by giving the example of a former employee who misappropriates a customer list and discloses it to his new employer (a competing firm).[1510] In this context, one could argue that the information is readily accessible on the Internet or telephone books and consequently it should not merit protection. According to Californian law, to avoid liability, the competing firm would always have to provide evidence that it conducted the search independently and gathered the relevant data without using the list compiled by the former employee. Risch understands that such an approach reduces the incentives of the owner to overprotect information and also redirects the incentives to research where it is cheaper to do so. At the same time, he suggests that it diminishes litigation costs and the associated uncertainty.[1511]

Similar arguments are raised by Unikel, who understands that the "not readily ascertainable by proper means" benchmark allows companies to deploy "improper short cuts" to obtain valuable information and avoid paying the cost of such labour, based on the mere fact that it was theoretically possible to obtain such knowledge through proper means.[1512]

Even though at first glance such propositions may seem sound, upon closer examination it seems unreasonable to demand that the defendant provide evidence that he in fact obtained the information independently. Such a reversal of the burden of proof seems unjustified and would allow for privatising information that is in fact already part of the public domain. Most importantly, it would spur abusive litigation. In addition, this is not supported by the TSD, which according to Article 11(1) TSD requires *the applicant* to prove in any case that: (i) the trade secret exists (i.e. the information complies with the requirements of protection); (ii) the applicant is the trade secret holder; and (iii) the trade secret has been ac-

1508 Michael Risch 2007 (n 15) 54.
1509 California Civil Code § 3426.1(d).
1510 This is largely based on the facts in *Abba Rubber Co. v. Seaquist,* 286 Cal.Rptr. 2d 518 (Cal. Ct. App. 1991).
1511 Michael Risch 2007 (n 15) 55.
1512 Robert Unikel, 'Bridging the "Trade Secret" Gap: Protecting "Confidential Information" Not Rising to the Level of Trade Secrets' [1998] 29 Loyola University Chicago LJ 841, 876.

quired unlawfully, is being unlawfully used or disclosed, or its unlawful acquisition, use or disclosure is imminent.[1513]

On a more general scale, the approach supported by Risch and Unikel assumes that the distinction between information generally known and easily accessible (or readily ascertainable) is a straightforward one. However, in practice it often appears to be a grey area. Indeed, even within the example proposed by Risch, it is possible to distinguish between different scenarios. On the one hand, if the disputed list concerns only the identification of all potential customers who appear in industry publications or catalogues, the content of the list should fall under the category of "readily accessible" information. In this case, it appears too burdensome to require the defendant to prove the independent generation of the information. By contrast, if the list includes references to the profitability or revenue generation gathered by the former employer over the course of his business with the investment of substantial labour and intellectual skill, the content of the list should be considered as not generally accessible (i.e. secret).[1514]

Against this background, Rowe[1515] draws a parallel with patent law and highlights that the "readily ascertainable" requirement includes "knowable but not yet generally known information" and therefore resembles the "in a printed publication" standard of patent law. According to the U.S. Supreme Court in *In re Leo M. Hall*, prior art includes "information that is sufficiently accessible, at least to the public interested in the art, so that such a one by examining the reference could make the claimed invention without further research or experimentation".[1516]

The above goes to show that it is not possible to extract a normative standard that allows for delineating with precision in all circumstances when information is readily accessible and when it maintains its secret nature. Such an assessment is to be conducted on a case-by-case basis. However, it is submitted that the deciding factor should be whether the investment of intellectual skill to gather or access the information concerned is necessary to gain actual knowledge of the "knowable information", that is, if the misappropriator has to use his rationality to gain knowledge of the information concerned, through a process of trial and error. Yet, such in-

1513 This is established as a maximum standard of protection, according to Article 1(1) TSD.

1514 James Pooley, 'The Uniform Trade Secrets Act: California Civil Code 3426' [1985] 1 Santa Clara High Technology LJ 193, 198 footnote 20.

1515 Elizabeth A. Rowe, 'Saving Trade Secret Disclosures on the Internet Through Sequential Preservation' [2007] 42 Wake Forest LR 1.

1516 *In re Leo M. Hall* 781 F.2d 897, 899 (Fed. Cir. 1986).

formation need not be novel, inventive or original.[1517] This should be viewed as an indicator that the information is secret and needs to be reverse engineered. For instance, in the case of perfumes, only a skilled chemist would be able to reconstruct the formula drawing from the analysis carried out by a gas-chromatograph spectrum after a process of trial and error to achieve the most similar results.

In practice, courts frequently rely on circumstantial evidence to assess whether information is readily apparent. This includes: (i) the steps adopted by the trade secret holder to protect the information, (ii) the difficulty for competitors to generate the same information, and (iii) the willingness of third parties to enter into licensing agreements to use the information.[1518]

In sum, the underlying reason behind the relative secrecy prong is that undisclosed information may confer upon its holder a competitive advantage and if a competitor wants to acquire it he must invest substantial time, effort and skill to do so.[1519] This is consistent with the incentives to innovate rationale: ultimately, the law of trade secrets protects investment in the creation of valuable information.[1520]

C) Fencing secrecy by its negative dimension

Drawing on the previous analysis, it can be concluded that not every disclosure renders a trade secret generally known or readily accessible and thus unprotectable. In fact, the level of publication required to destroy secrecy depends on a number of factors. The most important of these are the kind of information concerned, the relevant part of the public who is interested in learning the information, the place, form and extent of publication and the amount of time during which the information is accessible.[1521] Indeed, due to the absence of a normative standard, it appears that secrecy is better conceptualised by reference to its negative dimension in order to establish its boundaries with the public domain. With this in

---

1517 This is developed further in Chapter 4 § 4 E), where the secrecy standard is compared to other IRPs normative standards

1518 *Rockwell Graphic Systems, Inc. v. DEV Industries, Inc.,* 925 F.2d 174, 179 (7th Cir. 1991).

1519 Rudolf Kraßer 1977 (n 1327) 179.

1520 As argued in chapter 1 § 2 B) I.

1521 Paul Lavery, 'Secrecy, springboards and the public domain' [1998] 20 EIPR 93, 95; Lionel Bently and Brad Sherman 2014 (n 125) 1148.

mind, the following section looks first into the "Third Party Doctrine" of trade secrets law in an attempt to conceptualise the different types of disclosures, drawing from Sandeen's proposal,[1522] while section II examines the effect of specific disclosures with the purpose of identifying the guiding principles that should govern the assessment of whether information still retains its secret nature.[1523] In particular, section II intends to address the challenges raised by digital disclosures.

I. The "Third Party Doctrine" of trade secrets law and its limitations: conceptualising the different types disclosures

As outlined above,[1524] the relative secrecy requirement implies that it is possible that several persons can have access to the same information without it losing its secret nature. However, the trade secret holder must be careful when sharing such information, particularly outside the sphere of his business. According to the so-called "third-party doctrine", as conceptualised in the U.S., the mere imparting of a trade secret by its holder does not give rise to a duty of confidentiality. "It must be found in some other source of law".[1525] Indeed, pursuant to the prevailing case law in the U.S., a duty of confidentiality usually arises as a result of one of the following four situations: "(1) an express agreement; (2) an agreement implied-in-fact; (3) an agreement implied-at-law (a "quasi-contract"); or (4) a duty imposed by law either as specified in a statute (attorney-client privilege) or based upon commercial law principles".[1526] Similar considerations apply in England under the breach of confidence action, which requires that the information is "imparted in circumstances giving rise to an obligation of confidence".[1527] Likewise, in Germany, the UWG only affords protection against the unlawful acquisition, use and disclosure of information that is

1522 Sharon K. Sandeen, 'Lost in the Cloud: Information Flows and the Implications of Cloud Computing for Trade Secrets Protection' [2014] 19 Virginia JL & Technology 2.

1523 This section follows the structure implemented by James Pooley 2002 (n 66) § 4.04[2] 26 with some minor variations regarding Internet disclosures, cloud computing and the use of known information for an unkown use.

1524 See chapter 4 § 4 A).

1525 Sharon K. Sandeen 2014 (1522) 50.

1526 Sharon K. Sandeen 2014 (1522) 50.

1527 For a detailed overview of the circumstances under which an obligation of confidence arises, see chapter 3 § 3 C) II. 2.

kept secret as a result of the will of the owner.[1528] Consequently, Sandeen suggests that the salient issue in conceptualising secrecy is to identify whether sharing information with third parties that are under no confidentiality obligation automatically deprives it of its secret nature.[1529] This is particularly relevant in the digital age, as information is becoming increasingly vulnerable.

Against this background the author notes that the term "disclosure" is used in the law of trade secrets with a two-fold meaning: (i) as one of the conducts under which liability arises, together with acquisition and use,[1530] and (ii) as one of the acts that precludes trade secrets protection (secrecy-destroying acts), which can be carried out by the holder of the information, a misappropriator or any third party.[1531] In this context, she notes that the disclosure test is not just a de facto test; it has legal implications and therefore it is possible to conceptualise six types of secrecy-destroying disclosures, which are defined in narrow or broader terms based on the actors and circumstances involved.

- Type I disclosure encompasses the dissemination of information by a misappropriator. In such a context, Sandeen holds that courts should apply a narrow definition of disclosure in order to allow the trade secret owner to seek redress and prevent further dissemination of the information. The author further notes that courts in the U.S. are reluctant to consider the dissemination of information to a limited number of third parties that results from a misappropriation act as forfeiting trade secrets protection, so long as the information does not become generally known.[1532]
- Type II disclosures relate to accidental disclosures. According to the author, a narrow application of the term disclosure is supported by U.S. courts and the UTSA, by virtue of which the liability of third parties is established provided that they had knowledge of the accidental nature of the disclosure.[1533]
- Type III disclosures examine whether the information was "generally known" at the time that the misappropriation took place. This category

1528 Chapter 4 § 2 A) II. 4.
1529 Sharon K. Sandeen 2014 (1522) 50.
1530 See Article 4(3) TSD.
1531 Sharon K. Sandeen 2014 (1522) 65.
1532 Sharon K. Sandeen 2014 (1522) 65.
1533 Sharon K. Sandeen 2014 (1522) 66.

is conceptually broader than Type I and Type II, because there is no legal basis to restrict the use of what is "generally known".[1534]
- Type IV disclosures refer to "readily ascertainable" information that is excluded from the scope of protection of trade secrets and, just like Type III disclosures, these are conceptually broader than Type I and Type II.
- Type V disclosures encompasses information acquired by third parties through lawful means, such as reverse engineering and independent creations. In order to prevent overlaps with the patent system, Sandeen suggests that these types of disclosures are conceptually broader than the types of disclosures under sections I and II above.[1535]
- Type VI disclosures encompass "owner initiated disclosures" and accordingly should be conceptualised in the broadest sense, because in such a case the trade secret holder did not take the necessary steps to protect the information.[1536]

The analytical framework proposed by Sandeen provides an insightful scrutiny of the different categories of disclosures. However, it does not attach any legal consequences to the conceptualisation of disclosures as "broad", "broader", and "broadest", and, as a result, it does not create a normative standard that allows for delineating in a precise manner the contours of secrecy and the public domain. Indeed, the author expressly acknowledges that such an analytical model provides no insight into how to define disclosures with respect to trade secrets stored in the cloud.[1537] After all, as has already been argued, such an analysis is largely factually driven.

In the light of the shortcomings of the methodology proposed by Sandeen, this dissertation takes a case-oriented approach and examines specific types of disclosures and how case law in different jurisdictions has assessed their effects. Such an analysis ultimately intends to extract the guiding principles that may assist courts in determining whether a specific piece of information is part of the public domain in view of the harmonisation goals pursued by the TSD.

1534 Sharon K. Sandeen 2014 (1522) 67.
1535 Sharon K. Sandeen 2014 (1522) 67.
Sharon K. Sandeen 2014 (1522) 69-70.
1536 Sharon K. Sandeen 2014 (1522) 70.
1537 Sharon K. Sandeen 2014 (1522) 78-79.

II. Effects of the disclosure

1. Disclosure in a patent application or specification

a) England as an example case

Pursuant to Article 93 EPC, European Patent applications should be published at the latest eighteen months after the date of filing or before that day at the request of the applicant. Upon publication, the trade secrets described therein lose their confidential nature. This has been confirmed by both the Federal Supreme Court in Germany[1538] and the House of Lords in England,[1539] and it is also a well-established principle under U.S. Law.[1540] Notwithstanding this, it is also a general principle that secrets related to an invention that are not disclosed in the application shall remain secret.

The controversies that may arise in this context are best illustrated in the English case *Mustad&Son v Dosen and another*.[1541] There, the plaintiffs sought to restrain the defendant, one of their former employees, from communicating confidential information regarding the process of manufacturing a machine for the production of fishhooks. Shortly after the initiation of the proceedings, the plaintiffs filed for a patent application, which in essence covered the confidential information. Upon appeal, the House of Lords ruled that regardless of the validity of the patent, "the secret, as a secret had ceased to exist"[1542] as the patent specification had been published and therefore the plaintiffs were not entitled to obtain any injunction restraining the defendants from using what was "common knowledge". Remarkably, the court also accepted that in abstract it could be possible to protect ancillary secrets that had not been disclosed in the specification, even though in the present case the plaintiff had failed to provide evidence of the existence of such information.[1543]

Another highly contested issue is whether the publication of a foreign patent application or specification may affect the secret nature of information that was independently developed by the trade secret holder. In

---

1538 BGH GRUR 1975, 206, 208 – *Kunststoffschaum-Bahnen*.
1539 *Mustad v Son v Dosen and another* [1964] 1 WRL 109 (HL), 111.
1540 *Conmar Products Corp. v. Universal Slide Fastener Co.*, 172 F.2d 150, 155–156 (2d Cir.1949).
1541 *Mustad v Son v Dosen and another* [1964] 1 WRL 109 (HL), 111.
1542 *Mustad v Son v Dosen and another* [1964] 1 WRL 109 (HL), 111.
1543 *Mustad v Son v Dosen and another* [1964] 1 WRL 109 (HL), 111.

Franchi v Franchi,[1544] the High Court of Justice of England and Wales concluded that the publication of a patent specification in Belgium also rendered the information in the public domain in England, as patent attorneys regularly reviewed foreign publications.[1545] Conversely, in Germany the Federal Supreme Court reached a different conclusion in 1962 in the *Kieselsäure* decision, in which the validity of a licensing agreement was confirmed, despite the fact that the licensed secret process was the object of a U.S. patent published sometime after the agreement was concluded.[1546]

b) Guiding principles

In the light of the above, it is submitted that:

(i) The secrets enshrined in a patent specification are disclosed upon publication, but ancillary secrets that can only be devised with substantial intellectual skill retain their secret nature.

(ii) The withdrawal of an application prior to the eighteen months that precede the publication prevents the invention from entering the public domain. In such a case, secrecy is preserved.[1547]

(iii) Unlike the novelty prong in patent law, secrecy is not an absolute standard. However, published foreign patent applications and specifications will most likely be deemed secrecy destroying.[1548] Indeed, nowadays most patent offices have public databases available online, which allow any third party to access the published applications and specifications at no cost. In addition, these can be easily translated by automatic translation tools, allowing the recipient to get a very accurate insight into their content. During the last decade, the accessibility of obscure sources through the Internet has been widely discussed. Due to its practical importance, this topic is examined in greater detail in section 4 below.

1544 *Franchi v Franchi* [1967] RPC 149 (Ch).
1545 *Franchi v Franchi* [1967] RPC 149 (Ch).
1546 BGH GRUR 1962, 207, 211 – *Kieselsäure.*
1547 Pursuant to article 87(4) EPC; see furthermore Guidelines for Examination in the EPO. Part E. Chapter VIII. Section 8.1.
1548 *Ohly*/Sosnitza (n 813) § 17 Rdn 9.

2. Disclosure to the state and its authorities

In the XXI century, the smooth functioning of democratic states requires private companies and individuals to disclose vast amounts of data in the interests of transparency, safety and environmental protection. Both in the acquis communautaire and the national legal regimes a myriad of statutes have been enacted compelling undertakings to reveal a substantial amount of information (including trade secrets) to public authorities. This is regarded as an essential part of the democratic process.[1549] However, in the context of trade secrets, this leads to the question of whether such information is legally protected against subsequent unauthorised use or disclosure. Indeed, representatives of the perfume industry identified the disclosure of secret information to the state and its agencies as one of the main factors underlying the increasing leakage of trade secrets. This was also one of the main concerns raised by stakeholders during the negotiation of the TSD.[1550] To illustrate the legal issues that arise as a result of such disclosures, the English jurisdiction is taken as an example case of the conflicting interests that public authorities need to balance (section a). Next, the relevant provisions within the acquis communautaire (section b) and their intersection with the TSD are studied (section c). Finally, a number of guiding principles are formulated (section d). From the outset, it should be noted that this is a particularly complex topic that touches upon numerous fields of law, such as public law and data protection law. Consequently, this study is confined to the study of the effects of public bodies' disclosures from the angle of trade secrets protection.

a) England as an example case

In England, commentators and case law seem to agree on the fact that an obligation of confidence may arise with regard to information disclosed by individuals or companies to state agencies when it is conveyed on a voluntary basis (for example in connection to public procurement);[1551] or a compulsory basis (such as in the course of a competition or a police investiga-

1549 Tanya Aplin and others 2012 (n 22) para 13.164.
1550 See chapter 5 § 4 B) II.
1551 John Hull 1998 (1016) paras 4.105-4.109

tion),[1552] and also in order to meet certain statutory conditions.[1553] The latter case usually involves the disclosure of sensitive information to a state authority to support the application to obtain permission to carry something out, such as the marketing of a cosmetic product or a new drug.[1554] The scope of the obligation of confidence in the latter scenario was discussed in *Re Smith Kline French Laboratories Ltd*[1555] where the plaintiff, a pharmaceutical company, disclosed secret information to the Department of Health in order to obtain marketing authorisation for one of its drugs in the UK. After some time, it came to the attention of the plaintiff that the Department of Health intended to use the data submitted in order to assess the applications of its competitors. Consequently, the plaintiff brought legal action based on a breach of confidence. After a number of appeals, the House of Lords ruled that the Department of Health could make use of the information in the public interest to perform its tasks.[1556] However, the court added that disclosures to third parties would result in a breach of confidence.[1557]

The above goes to show that if no express obligation of confidence between the disclosing party and the recipient authority exists, its scope should be inferred from the circumstances of the case. In particular, in *Re Smith Kline French Laboratories Ltd*[1558] the House of Lords argued that special attention should be paid to the role and purposes of the recipient authority.[1559] Hence, it was concluded that the Department of Health was entitled to use the data to perform any of "its functions" as per the relevant legislation.[1560]

In addition, confidentiality obligations have also often been tempered by the public interest defence, mostly with regard to safety and health, which may override any inter partes obligations of confidence.[1561] More

1552 This was the case in *Marcel v Commission of Police of the Metropolis* [1992] Ch 225 (CA).
1553 Tanya Aplin and others 2012 (n 22) para 13.164.
1554 John Hull 1998 (1016) paras 4.105- 4.109.
1555 *Re Smith Kline & French Laboratories Ltd* [1990] 1 AC 64 (HL).
1556 *Re Smith Kline & French Laboratories Ltd* [1990] 1 AC 64 (HL), 98E.
1557 *Re Smith Kline & French Laboratories Ltd* [1990] 1 AC 64 (HL), 98E.
1558 *Re Smith Kline & French Laboratories Ltd* [1990] 1 AC 64 (HL).
1559 Tanya Aplin and others 2012 (n 22) para 13.30.
1560 *Re Smith Kline & French Laboratories Ltd* [1990] 1 AC 64 (HL), 82.
1561 Tanya Aplin and others 2012 (n 22) para 13.37.

generally, no breach of confidence exists if the disclosure of information is mandated (or envisaged) in a statute or by a court order.[1562]

As a corollary of the public interest defence and in order to ensure transparency within democratic societies, states and their agencies are frequently under an obligation to disclose information under their control to third parties. This often conflicts with the confidentiality obligations imposed by law or agreed upon contractually between the receiving authority and the party that submits the information.[1563] Such a tension arises mostly with regard to the access rights of the data subject with respect to his personal data (according to the applicable data protection legislation) and the right of citizens to access information under the control of the state. Providing an analysis of the former case exceeds the scope of the present research. Consequently, the remainder of this section looks into the effects on trade secrets protection in the latter case, and particularly under the legal framework created by the Freedom of Information Act.[1564]

The Freedom of Information Act came into force on 1 January 2005 and, in essence, it introduced for the first time a statutory right to access information held by public authorities.[1565] The right covers all information, irrespective of its format and when it was submitted or created.[1566] As a result, public authorities are compelled to publish the information that they hold if requested to do by any third party (individuals or legal entities). Failure to comply with such a request within twenty days from the day of receipt[1567] may be appealed in the first instance before the Information Commissioner[1568] and in the second instance before the Information Tribunal.[1569]

However, the Act provides for a number of exemptions to the disclosure of information in order to ensure the protection of other potential conflicting interests. These exemptions are regulated in Part II of the Act and can be grouped into four main areas: (i) information that is already available to the third party; (ii) information on matters of public importance

1562 John Hull 1998 (1016) paras 4.109 - 4.101.
1563 Tanya Aplin and others 2012 (n 22) para 13.103.
1564 Freedom of Information Act 2000 (FOIA).
1565 Karen McCullagh, 'A tangled web of access to information: reflections on R (on the application of Evans) and another v Her Majesty's Attorney General' [2015] 21 European J of Current Legal Issues.
1566 Ibid.
1567 FOIA 2000, s 10.
1568 FOIA 2000, s 18.
1569 FOIA 2000, s 57.

(such a state defence or economic welfare); (iii) information that may prejudice private interests (as would be the case of trade secrets); and (iv) information prohibited by statute.[1570] The third category is of particular relevance for the purposes of the present research as it includes breach of confidence (s 41) and trade secrets and commercial prejudice (s 43).

The exemption set out in s 41 FOIA provides that public authorities shall not publish the information requested if this would result in a breach of confidence. More specifically, the literal wording of the provision precludes the disclosure of information if:

(a) it was obtained by the public authority from any other person (including another public authority), and
(b) the disclosure of the information to the public (otherwise than under this Act) by the public authority holding it would constitute a breach of confidence actionable by that or any other person.[1571]

The breach of confidence exemption is absolute in nature, which means that if it is applicable, the competent authorities shall not take into account other public interests.[1572] Notwithstanding this, courts have interpreted the requirement of "obtention" as not including information disclosed in the context of contractual relationships, such as in the case of public procurement.[1573] Consequently, the disclosure of sensitive data in contracts that involve public authorities shall be subsumed under the exemption set out in s 43 FOIA (commercial interest).[1574]

The commercial interest exemption provides a qualified exception regarding the publication of two categories of information: (i) trade secrets and (ii) information, the disclosure of which would "prejudice the commercial interests of any person (including the public authority holding it)".[1575] Pursuant to the Information Tribunal the term treade secret includes "something technical, unique and achieved with a degree of diffi-

1570 Tanya Aplin and others 2012 (n 22) para 13.115.
1571 FOIA 2000, s 41.
1572 Tanya Aplin and others 2012 (n 22) para 13.130.
1573 John Macdonald and Ross Crail, *John Macdonald on the Law of Freedom of Information* (3rd edn, OUP 2016) para 5.94.
1574 Notwithstanding this, John Macdonald and Ross Crail, *John Macdonald on the Law of Freedom of Information* (3rd edn, OUP 2016) para 5.408 note that presumably the majority of the information that would hinder commercial interests will also be regarded as confidential information and therefore, be subject to the exemption established in s 41 FOIA 2000, which is absolute in nature.
1575 FOIA 2010, s 43; John Macdonald and Ross Crail, *John Macdonald on the Law of Freedom of Information* (3rd edn, OUP 2016) para 5.398

culty and investment".[1576] It refers to the "highest level of secrecy".[1577] By contrast, the second category refers to disclosures that would create a commercial prejudice of any sort, including an increase in the price of a service provided to a public authority or the commercial reputation of a company.[1578] In cases where the nature of the specific piece of information is not clear, the Information Tribunal has subsumed it under the commercial interest category as "commercially sensitive" information.[1579]

However, due to the qualified nature of the exemption under s 43 FOIA, even if the requested information falls into one of the two categories referred to in the provision, the public authorities have to consider whether "the public interest in maintaining the exemption outweighs the public interest in disclosing the information", as per section 2(2)(b) FOIA. In particular, the value of the secret and the likelihood that the publication of the information will cause commercial prejudice are weighed against the public interest in transparency.[1580] In *DWP v IC*,[1581] a case concerning the disclosure of a financial model of a Government IT service provider, the Information Tribunal held that such information constituted a trade secret and that "if the information is a trade secret there is a strong public interest in protecting such a secret" because disclosure will not only negatively affect the holder's business, but will also provide competitors with an unfair commercial advantage.[1582]

In the light of the foregoing, it appears that according to the FOIA, in the case of trade secrets and other commercial information, public authorities are always requested to balance the conflicting interests before publishing the information requested.[1583] In particular, in the case of trade secrets, courts seem to recognise a strong public interest in their protection. However, such a principle is not uniformly acknowledged or applied across the

1576 *Department of Health v Information Commissioner* (EA/2008/0018, 18 November 2018) [52].
1577 *Department of Health v Information Commissioner* (EA/2008/0018, 18 November 2018) [53].
1578 Tanya Aplin and others 2012 (n 22) para 13.132.
1579 *Department of Health v Information Commissioner*, (EA/2008/0018, 18 November 2018) [54].
1580 Tanya Aplin and others 2012 (n 22) para 13.137.
1581 *DWP v IC* (EA/2010/0073, 20 September 2010).
1582 *DWP v IC* (EA/2010/0073, 20 September 2010) [84].
1583 John Macdonald and Ross Crail, *John Macdonald on the Law of Freedom of Information* (3rd edn, OUP 2016) para 16.13.

myriad of statutes that regulate the disclosure of information held by public authorities to third parties.[1584]

b) Confidentiality in the acquis communautaire and the right of access to documents

The principle of confidentiality has been incorporated into the acquis communautaire by virtue of Article 339 TFEU, which provides that:

> The members of the institutions of the Union, the members of committees, and the officials and other servants of the Union shall be required, even after their duties have ceased, not to disclose information of the kind covered by the obligation of *professional secrecy*, in particular information about *undertakings*, their *business relations* or their *cost components* (emphasis added).

It is also embedded in the ChFREU, which enshrines the principles of respect for private life (Article 7 ChFREU) and protection of personal data (Article 8 ChFREU).

In turn, such a principle has been included in a number of legal provisions of secondary EU law. For instance, in the context of competition investigations, Article 28(2) of Regulation 1/2003[1585] notes that the national and EU Competition authorities and their employees shall not disclose information "covered by the obligation of professional secrecy".

However, the observance of confidentiality is not absolute, but is subject to numerous statutory limitations that mostly follow an unsystematic approach.[1586] Just as in the UK, in the EU the general principle of confidentiality has been tempered by the right of access to documents that it is also part of the acquis communautaire, pursuant to Article 42 ChFREU and Article 15(3) TFEU. A particularly notable manifestation of this principle is Regulation 1049/2001 regarding public access to European Parliament, Council and Commission documents,[1587] which was adopted in order to

---

1584 Tanya Aplin and others 2012 (n 22) para 13.137.

1585 Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty [2003] OJ L1/1.

1586 Tanya Aplin and others 2012 (n 22) para 13.1150.

1587 Regulation of the European Parliament and of the Council (EC) 1049/2001 of 30 May 2001 regarding public access to European Parliament, Council and Commission documents [2001] OJ L145/43 (Regulation 1049/2001).

lay down the legal framework that governs the right to access documents disclosed to the Commission, the European Parliament and the Council of the EU and to safeguard transparency during the decision-making processes of these institutions, in line with the objectives pursued by the FOIA in England.[1588]

In particular, Article 4 of Regulation 1049/2001 provides that the exercise of the right of access is subject to a number of exceptions. Specifically, pursuant to paragraph 1 of Article 4(2) of Regulation 1049/2001, access can be rejected if it would weaken the protection of "commercial interests of a natural or legal person, including intellectual property". The extent to which the reference to intellectual property encompasses trade secrets is uncertain, as examined above.[1589] However, it is undisputed that trade secrets fall under the scope of protected "commercial interests".[1590] This was the approach adopted by the CJEU in the *European Commission v Agrofert Holding a.s* case,[1591] where the court upheld a decision by the Commission in which access to a number of documents disclosed by the notifying parties during the course of a merger control process was denied to a third party ("Agrofert") that had requested it. In its legal reasoning, the Commission invoked paragraph 1 of Article 4(2) of Regulation 1049/2001 to deny access because the information requested was "commercially sensitive information relating to the commercial strategies of the notifying parties, their sales volumes, their market shares or customer relations", but no reference to trade secrets was made.[1592] Upon appeal, the CJEU held that the interpretation of paragraphs 1 and 3 of Article 4(2) established a general presumption "that the disclosure of the documents concerned undermines, in principle, the protection of the commercial interests of the undertakings involved in the merger and also the protection of the purpose of investigations relating to the control proceedings".[1593]

1588 Case C–404-10 P *Lagardère SCA v Éditions Odile Jacob SAS* (CJEU, 29 June 2012) para 109; John Macdonald and Ross Crail, *Macdonald on the Law of Freedom of Information* (3rd edn, OUP 2016) para 11.14.

1589 See chapter 1 § 3 B) I. 4.

1590 Tanya Aplin and others 2012 (n 22) para 13.171.

1591 Case C–477/10 P *European Commission v Agrofert Holding a.s*. (CJEU, 28 June 2012).

1592 Case C–477/10 P *European Commission v Agrofert Holding a.s*. (CJEU, 28 June 2012) para 10.

1593 Case C–477/10 P *European Commission v Agrofert Holding a.s*. (CJEU, 28 June 2012) para 64.

However, in a more recent decision concerning the disclosure of the clinical study report in the Marketing Authorisation application dossier for a medicinal product (Translanta) by the European Medicines Agency, the GCEU noted that clinical study reports do not enjoy a general presumption of confidentiality based on the implicit ground that they are "as a matter of principle and in their entirety, clearly covered by the exception relating to the protection of commercial interests of (market authorisation applicants)".[1594] The GCEU therefore held that in the assessment of whether the exception set out in the first indent of Article 4(2) of Regulation 1049/2001 may prevent the disclosure of information, the European Medicines Agency must conduct "a concrete, individual examination of each document in the application file for (Marketing Authorisation)".[1595] Indeed, the existence of such a general presumption was also denied by the GCEU with regard to a report on chemical safety submitted to the European Chemical Agency, which was requested by a competitor, also on the basis of Regulation 1049/2001.[1596]

c) Protection of competing interests in the TSD

The competing interest between the protection of valuable commercial information held by a company and the general interest in transparency and access to documents outlined in the previous sections is also apparent in a number of provisions of the TSD. On the one hand, Article 1(2)(b) stipulates that the TSD should not affect those provisions of national and EU Law that mandate the disclosure of information (including trade secrets) to the general public or to public, administrative or judicial authorities. In this regard, Recital 11 specifically indicates that the provisions of the TSD should not affect the application of EU and national rules that demand the

1594 Case T–718/15 *PTC Therapeutics International Ltd v EMEA* (GCEU, 5 February 2018) para 53.

1595 Case T–718/15 *PTC Therapeutics International Ltd v EMEA* (GCEU, 5 February 2018) para 53.

1596 Case T–189/14 *Deza v ECHA* (GCEU, 13 January 2017) para 40: "No general presumption can therefore be inferred from the provisions of Regulation No 1907/2006. It cannot therefore be accepted that, in the context of an authorisation procedure provided for by Regulation No 1907/2006, the documents communicated to the ECHA are to be regarded as being, in their entirety, clearly covered by the exception relating to the protection of the commercial interests of applicants for authorisation".

disclosure of trade secrets to public authorities and that allow or require any subsequent disclosure and, in particular, the access to document rights set out in Regulation 1049/2001. Similarly, Article 1(2)(c) sets forth that the rules laid down in the TSD should not interfere with other national or Union law provisions that mandate or allow the disclosure of any information about businesses to public institutions, bodies and authorities in accordance with national or EU law.[1597] More generally, Article 3(2) stipulates that when the acquisition, use or disclosure of a trade secret is laid down either in national or union law provisions, it should be deemed lawful. In contrast, Recital 18 indicates that this should not be to the detriment of the obligation of confidentiality imposed on the acquirer or recipient of the information, either by national or by EU law. Most notably, this recital specifies that the Directive does not exonerate public authorities from obligations of confidence with regard to information submitted by the trade secret holder and mentions, as an example, the information acquired by contracting authorities in the course of public procurement procedures.[1598]

d) Guiding principles

In the light of the foregoing analysis, identifying the effect of disclosures compelled by public authorities is not straightforward, as an array of interests and legal provisions of constitutional, public and private law come into play. Notwithstanding this, the following interpretive principles are submitted:

(i) The "commercial interests (…) including intellectual property" exemption established in Article 4(2) of Regulation 1049/2001 should be deemed to include trade secrets, pursuant to the definition stipulated in Article 2(1) TSD, which is now part of the acquis communautaire.

(ii) In line with the principles that inform the practice of the CJEU with regard to the first indent of Article 4(2) of Regulation 1049/2001, the disclosure of trade secrets submitted to public authorities that is mandated or allowed by national or EU legislation and that may be subject to limitations on the basis of a commercial interest or an intellectual property right of the holder, as set out in the relevant statute, should be assessed on a case-by-case basis, in accordance with the specific cir-

1597 See Recital 11 TSD.
1598 See Recital 18 TSD.

cumstances of the case. In particular, if the disclosure of the information could cause irreparable harm to the holder, public authorities should consider whether providing partial disclosures or redacted versions could also serve public transparency purposes and protect the business interest of the parties. In such a context, it is submitted that the trade secrets holders should always be notified of the request for information by the third party or its publication and be given an opportunity to present the pertinent arguments.

(iii) If the relevant statutes set out an obligation of confidence on a national or EU authority or public body that is not observed, the said authority or public body shall be deemed liable for unauthorised use or disclosure of a trade secret. If no such obligation is stipulated, the acquisition, use and disclosure of the trade secret mandated or allowed by EU law should be considered lawful, in accordance with Article 3(2) TSD.

In sum, due to the overlap of provisions and legal interests that come into play, it is likely that further guidance from the CJEU will be sought, in line with the series of decisions rendered by the CJEU with respect to the first indent of Article 4(2) of Regulation 1049/2001.

3. Marketing of a product in which the trade secret is embodied

In the course of misappropriation proceedings, defendants frequently counter-claim that no such misappropriation existed, because the information lacked the necessary quality of confidence. Most frequently, they argue that by placing a product on the open market in which the trade secret was embodied, the plaintiff made it generally available, thereby preventing trade secrets protection. This section intends to map out the general principles that govern such an appraisal following the methodology of comparative law. The general proposition in the U.S. and Germany[1599] is that marketing a product, as such, does not necessarily reveal all of the trade secrets associated with it. In England, commentators and case law have not provided a uniform solution, but the prevailing view is that a certain amount of disclosure is permitted.[1600] Each of these jurisdictions is analysed in turn.

1599 Rudolf Kraßer 1970 (n 831) 590; RGZ 1935 149, 329, 330 – *Stiefeleisenpresse*.

1600 The English case law is stricter than the German and U.S. jurisprudence on this topic; as examined in chapter 6 § 2 B) below dealing with reverse engineering; for an analysis of the English approach see Tanya Aplin, 'Reverse Engi-

a) U.S.

In the U.S., two of the main legislative sources for trade secrets protection, namely the UTSA and the Restatement (Third) of Unfair Competition, note that the marketing of a product in which a trade secret is embodied does not automatically deprive the information of its concealed nature, as long as substantial investment, time and effort are necessary to obtain it[1601] and the recipient is under no obligation of confidence.[1602] This signals that the information is subject to a process of reverse engineering and therefore it is not generally known or readily ascertainable.

Such a proposition has been restated in numerous decisions. For instance, as early as 1951, the Supreme Court of Texas held that the idea of a "metallic fishing rod that would collapse into once piece and thus serve as a walking stick"[1603] was based on "obvious" mechanical principles and could be easily imitated by "any reasonably experienced machinist that might see one for the first time or purchase it on the open market". Consequently, the Supreme Court of Texas ruled that the exhibition of the device to the public by "advertisement or sale" prevented trade secrets protection.[1604] Similarly, in 1964, the Court of Civil Appeals of Texas in El Paso held that an advertisement plan consisting of bonus cards with money amounts printed around the periphery of the card, which had been prepared by an advertising agency for the sole purpose of promoting sales in the grocery store, could not be considered a trade secret. In this respect, the court noted that the idea of punch cards was not new, as in fact similar cards were being used at the time of the alleged misappropriation in other

---

neering and Commercial Secrets' [2013] 66 Current Legal Problems 341, 347-348; *Franchi v Franchi* [1967] RPC 149 (Ch), 152.

1601 See UTSA Comment § 1: "Often, the nature of a product lends itself to being readily copied as soon as it is available on the market. On the other hand, if reverse engineering is lengthy and expensive, a person who discovers the trade secret through reverse engineering can have a trade secret in the information obtained from reverse engineering"; Restatement (Third) of Unfair Competition §39 (Am. Law Inst. 1995) comment f, Reporter's Note: "Public sale of a product does not preclude continued protection against the improper acquisition or use of information that it is difficult, costly, or time-consuming to extract through reverse engineering"; James Pooley 2002 (n 66) § 4.04 [3]4-34, 4-35.

1602 Gale R. Peterson, 'Trade Secrets in an Information Age' [1995] 32 Houston LR 385, 450.

1603 *Wissman v. Boucher*, 240 S.W.2d 278, 278 (Tex. 1951).

1604 *Wissman v. Boucher*, 240 S.W.2d 278, 278 (Tex. 1951).

cities or states. Hence, the court concluded that the cards themselves were "self-explanatory on the face".[1605]

By contrast, U.S. courts held that the formula of a jet ink acquired by an employee during the course of his employment relationship was secret, despite the fact that the jet ink had been marketed for some time before the alleged misappropriation took place. According to the deciding court, the specific composition of the jet ink was not known to others in the industry and steps had been taken to preserve its confidential nature (through employment agreements). In addition, the value and the time and effort spent in developing the jet ink formula was undisputed and, consequently, it was noted that "duplication was not so simple as to deprive (the jet ink) of trade secret status".[1606] Nevertheless, it was further suggested that "a few sophisticated competitors may have had the resources to analyse and reproduce the series 400 inks by fair means" but this did not protect the defendant, who was found liable for trade secret misappropriation.[1607] Similar principles were restated in another case decided by the Appellate Court of Illinois, where loss of secrecy was linked to the possibility of duplicating the marketed products without "time consuming and expensive analysis of products in the public domain".[1608] In *Q-CO Industries, INC. v. Hoffman*, the New York Southern District Court ruled that computer programs were eligible for trade secrets protection.[1609] In particular, the court noted that the source code of the alleged misappropriated software was not accessible to the public, because the version commercially sold was copy protected, thereby preventing users from accessing it.[1610] In this regard, the court noted that, "secrecy will not be destroyed by the wide distribution of computer programs if they are distributed in object form only".[1611] Similarly, in *Epic Syst. Corp. v. Tata Consultancy Servs*, a jury regarded that the plaintiff's medical record software and related documents constituted a trade secret,

1605 *Furr's Inc. v. United Speciality Advertising Co*., 338 S.W.2d 762, 764 (Tex. App. 1960).
1606 *American Can Co. v. Mansukhami*, 728 F.2d 818, 819-820 (7th Cir. 1982).
1607 *American Can Co. v. Mansukhami*, 728 F.2d 818, 820 (7th Cir. 1982).
1608 *Colony Corp.of America v. Crown Glass Corp*, 430 N.E.2d 225, 227 (Ill. App. Ct.1981).
1609 *Q-CO Industries, INC. v. Hoffman*, 625 F.Supp. 608 (S.D.N.Y. 1985).
1610 *Q-CO Industries, INC. v. Hoffman*, 625 F.Supp. 608, 617-618 (S.D.N.Y. 1985).
1611 *Q-CO Industries, INC. v. Hoffman*, 625 F.Supp. 608, 618 (S.D.N.Y. 1985).

even though they were accessible to more than three hundred thousand users upon introducing the user credentials.[1612]

Importantly, a number of decisions in the U.S. have explored the concealed nature of trade secrets embedded in mass-distributed software, where concluding individual licensing agreements with users is not viable.[1613] For instance, In *Data Gene Corp. v. Digital Computer Controls Inc.* the plaintiff manufactured a new personal computer (Nova 1200), which was sold along with the engineer's drawings to allow the purchaser to do his own maintenance and repairs. The defendant, a hardware company, purchased a computer from the plaintiff (Data) and duplicated it with the aid of the diagrams provided along with the Nova 1200 minicomputer. While the parties agreed that the defendant was free to reverse engineer the lawfully purchased Nova 1200 computer, controversy arose with respect to the use of the drawings, as Data's standard contract form contained a confidentiality clause regarding the use of drawings, which was limited to maintenance, as opposed to manufacture. Such a possibility was expressly forbidden without the plaintiff's consent in writing.[1614] In view of the measures implemented by the plaintiff and the fact that the drawings had been distributed under an obligation of confidence, the Court of Chancery of Delaware ruled that the drawings retained their secret nature and the plaintiff prevailed in his claim. In this context, it was deemed that confidentiality had subsisted, although the defendant noted that at the time of the misappropriation, the drawings were available to almost six thousand users.[1615] In another case, *Data General Corp. v. Grumman Systems* the court concluded that the alleged misappropriated software remained secret because the licensing agreement included confidentiality and return upon non-use clauses.[1616] Yet, this has not been without criticism, particularly due to the potential pre-emptive effect that the Copyright Act may

1612 *Epic Systems Corporation v. Tata Consultancy Services Limited et al*, No. 3:2014cv00748 - Document 243 (W.D. Wis. 2015).

1613 Gale R. Peterson 1995 (n 1602) 449; see Michael Risch, 'Hidden in Plain Sight' [2016] 31 Berkeley Technology LJ 1635, 1649-1651 noting that in numerous decisions courts in the U.S. have ruled that software delivered to vendors or shown publicly had not been legally disclosed for the purposes of assessing secrecy.

1614 *Data Gene Corp. v. Digital Computer Controls Inc.*, 297 A.2d 437, 439 (Del. 1972).

1615 Miles R. Gilburne and Ronald L. Johnston, 'Trade Secret Protection for Software Generally and in the Mass Market' [1981] 3 Computer LJ 211, 230.

1616 *Data General Corp. v. Grumman Systems Support Corp.*, 36 F.3d 1147, 1167-1170 (1st Cir. 1994).

have over contractual obligations of confidentiality regarding computer programs, and especially with respect to shrink-wrap licenses.[1617] These are presented in many forms, but usually include a prohibition on reverse engineering the licensed software and become effective when the user breaks the seal or packaging in which the physical program is sold.[1618]

In sum, it appears that courts in the U.S. mostly understand that placing a product on the open market does not necessary render all of the trade secrets generally known or readily apparent, unless they can be devised upon inspecting the product with little effort.

b) England

In England, a review of the decisions that deal with the issue of whether the mere marketing of a product deprives the trade secrets embodied therein of their confidential nature also seems to indicate that a certain amount of circulation is permitted.[1619]

Such a principle appears in *Ackroyds (London) Ltd. v Islington Plastics Ltd.*[1620] In this case the defendants, plastic moulds manufacturers, entered into a contract with the plaintiff for the manufacturing of plastic swizzle sticks in the form of a Neptune's trident, based on a pattern designed by the plaintiff. Subsequently, they went on to manufacture the same tool for one of the plaintiff's main competitors. When the plaintiff found out, he decided to bring legal action against the defendant for an alleged breach of contract, as well as a breach of confidence. In the legal reasoning, with respect to the issue of confidentiality, Harver J noted that:

> (…) the mere publication of an article by manufacturing it and placing it upon the market, whether by means of work done on it or calculation or measurement which would enable information to be gained, is not necessarily sufficient to make such information available to the public. The question in each case is: Is such information available to

1617 Gale R. Peterson 1995 (n 1602) 449-450; the validity of shrink-wrap licenses has been highly contested. In this regard, see Mark A. Lemley, 'Intellectual Property and the Shrinkwrap Licenses' [1995] 68 Southern California LR 1239.

1618 Mark A. Lemley 1995 (n 1617) 1241.

1619 John Hull 1998 (n 1016) para 3.36; Tanya Aplin 2013 (n 1600) 347-348.

1620 *Ackroyds (London) Ltd v Islington Plastics Ltd* [1962] RPC 97 (Ch).

> the public? It is not, in my view *if work would have to be done upon it to make it available* (emphasis added).[1621]

As is apparent from the above, the critical factor was whether intellectual work was necessary to devise the secret information embodied in the marketed product, which ultimately led to the affirmation of the confidential nature of the pattern designed by the plaintiff. Similar principles were restated in *Alfa Laval v Wincanton,* which concerned the confidential nature of design drawings for a cheese block former machine.[1622] In the 1970s the defendant invented a cheese block former machine and some years later he assigned all of the intellectual property rights over the said machine to the plaintiff, including patents, copyright and trade secrets. However, by virtue of an agreement entered into by the plaintiff and the defendant in 1987, the defendant ceased to be involved in the design of the machines and became a mere manufacturer. At the same time, he undertook strict confidentiality obligations. A year later, the agreement was terminated and, subsequently, the defendant announced his intention to design and manufacture his own machine. Consequently, the plaintiff applied for a preliminary injunction on the basis of an alleged copyright infringement, misuse of confidential information and breach of contract. As regards the misuse of confidential information claim, Morrit J noted that confidentiality only persisted regarding the inner lining of the machine, which needed to be dismantled. However, he concluded that the external pipes could not be considered confidential, as they were "plain for everyone to see" upon marketing the product.[1623]

More recently, Arnold J had to decide whether the design of a half-size wind tunnel model of a Formula 1 racing car designed for one of the teams (Force India) was of a confidential nature, despite the fact that photographs of the vehicles had been published and certain parts had been sold by a Formula 1 memorabilia company. In deciding on the confidential status of information, he noted that:

> In cases concerning design drawings (…) much will depend on the level of generality of the information asserted to be confidential. If the claimant contends that information relating to the shape and configu-

---

1621 *Ackroyds (London) Ltd v Islington Plastics Ltd* [1962] RPC 97 (Ch), 104.

1622 *Alfa Laval Cheese Systems Ltd and Another v Wincanton Engineering Ltd* [1990] FSR 583 (Ch).

1623 *Alfa Laval Cheese Systems Ltd and Another v Wincanton Engineering Ltd* [1990] FSR 583 (Ch), 591.

> ration of the article depicted in the drawings is confidential, but the shape and configuration of the article can readily be ascertained from inspection of examples of the article which have been sold or are otherwise publicly accessible, then the claim will fail. If, on the other hand, the claimant contends that detailed dimensions, tolerances and manufacturing information recorded in the drawings are confidential, that information cannot readily be ascertained from inspection, *but only by a process of reverse engineering and the defendant has used the drawings as a short cut rather than taking the time and effort to reverse engineer*, then the claim will succeed (emphasis added).[1624]

In this context, the deciding judge held that the basic shapes of some of the parts of the Formula One cars were part of the public domain because they were ascertainable from pictures, but specified that the precise dimensions of specific parts remained concealed. Consequently, he concluded that the defendant's employees had indeed copied confidential material belonging to Force India, which the latter had supplied to the defendant for the provision of the agreed services.[1625] This finding was subsequently upheld by the Court of Appeal of England and Wales.[1626]

In the light of the above, it seems that English courts understand that the information embodied in a market product loses its secret nature if it can be obtained without the need to undergo a process of reverse engineering, that is, if no intellectual skill is necessary to devise the secret information.[1627] We will return to reverse engineering in chapter 6 as one of the main limitations of the rights conferred to the trade secret holder.[1628]

c) Germany

In Germany, the prevailing view is that the marketing of a product does not necessarily reveal all of the trade secrets embedded therein. This was stated, for instance, by the Bavarian Higher Regional Court, in a dispute

---

1624 *Force India Formula One Team Ltd v 1 Malaysia Racing Team SDN BHD* [2012] EWHC 616 (Pat) [221].
1625 *Force India Formula One Team Ltd v 1 Malaysia Racing Team SDN BHD* [2012] EWHC 616 (Pat) [280],[282],[290].
1626 *Force India Formula One Team Ltd v 1 Malaysia Racing Team SDN BHD* [2013] EWCA civ 780 (CA).
1627 Tanya Aplin 2013 (n 1600) 349.
1628 Chapter 6 § 2 B) III. 3.

concerning the unlawful acquisition of a computer program incorporated into a slot machine used for gambling purposes.[1629] According to the fact-pattern of the decision, the defendant, one of the users of the slot machines, managed to decompile the computer program after using the machine several times.[1630] In this context, the court ruled that even though the slot machines had been placed on the market[1631] and that the information could be obtained after investing 70 hours of work and 5.000 German Franks (2.500€), the information remained concealed.[1632] The High Court in Bavaria concluded that it was only accessible with great difficulty and cost, which was identified as the benchmark that signals the existence of a secret worth protecting. Then, the court went on to examine whether the act of reverse engineering should be considered lawful. Consequently, under German law, information remains secret if it can only be obtained with the investment of substantial skill and labour. In particular, secrecy has been construed in a very broad sense vis-à-vis reverse engineering, as examined in chapter 6.[1633]

d) Guiding principles

The comparative analysis conducted above reveals that in the three jurisdictions studied a certain level of circulation is permitted; secrecy is not necessarily lost by placing a product on the market. However, it is crucial to differentiate between two types of information: (i) information about the *development* and *production* of the product concerned, and (ii) information about its *actual configuration*.[1634]

The first category refers, for example, to the secret drawings containing the precise dimensions of specific moulds used to manufacture specific

1629 BayObLG GRUR 1991, 694 – *Geldspielautomat.*
1630 BayObLG GRUR 1991, 694, 697 – *Geldspielautomat.*
1631 BayObLG GRUR 1991, 694, 695 – *Geldspielautomat* noting that "Der Geheimnischarakter der Bauart einer Maschine, oder, wie hier, der Gestaltung des Computerprogramms eines Spielautomaten, wird auch nicht dadurch aufgehoben, daß die Geräte vom Hersteller veräußert werden" and that "Kenntnis, die sich der Täter nur durch Einsatz von 70 Beobachtungsstunden und 5 000, - DM Spielgeld verschaffen kann, wird nicht 'ohne größere Schwierigkeiten und Opfer' erlangt".
1632 BayObLG GRUR 1991, 694, 697 – *Geldspielautomat.*
1633 See Chapter 6 § 2 B) III. 3).
1634 James Pooley 2002 (n 66) § 4.04 34-35.

parts of a marketed product.[1635] In this case, the information remains secret so long as the analysis of the marketed product does not disclose the dimensions of the moulds. In the second category, the information about the internal configuration of the good (internal secrets) and its functionality may not be apparent upon examination, which confers its holder a lead time advantage when compared to the rest of competitors. It remains secret and therefore protectable until it is reverse engineered.[1636] Prime examples of the latter would be a chemical formula to produce rubber goods or encrypted information embedded within a vending machine.

A similar approach has also crystallised in consistent case law from the Boards of Appeal of the EPO with regard to the assessment of novelty. As outlined in chapter 1, while examining the interplay between trade secrets and patent rights, placing a product on the open market for which patent protection is later sought is only novelty destroying if it is possible for members of the public to acquire knowledge of that subject matter on the relevant priority day. This includes the external examination of the product, as well as the obtention of the invention after further analysis of the intrinsic features (those that do not need to interact with external conditions to become apparent).[1637]

The availability of an invention embodied in a marketed product was discussed by the Enlarged Board of Appeal of the EPO in the landmark decision G-1/92. In this case, it was considered whether the chemical composition of a product is part of the state of the art when the product in which it is embodied is marketed and can be analysed and reproduced by a skilled person.[1638] In delivering its decision, the Board started by noting that one of the main goals of any technical teaching is to allow any person with ordinary skills in the art to "use" or "produce" the product concerned. To that end, he would have to use "the general technical knowledge to gather all information enabling him to prepare the said product". In such a case, if the skilled person could find out the composition or the internal structure of the product and was able to reproduce it, it should be deemed that both the product and its composition or internal structure are

1635 *Ackroyds (London) Ltd. v Islington Plastics Ltd* RPC 97.
1636 James Pooley 2002 (n 66) § 4.04 34-35.
1637 See Guidelines of Examination in the EPO. Part G. Chapter IV. Section 7.2.; on the interpretation of the availability to the public of an invention by use followed by the Enlarged Board of Appeal of the EPO, G 1/92 [1993] OJ EPO 278.
1638 G 1/92 [1993] OJ EPO 278.

part of the state of the art.[1639] Based on the above premise, the Enlarged Board of Appeal concluded that the relevant yardstick is whether the information is accessible in a "direct" and "unambiguous" manner, not whether there is a reason to "look for it".[1640] Thus, under patent law marketing, a product in which an invention is embodied does not implicitly reveal anything beyond its composition or internal structure. Indeed, extrinsic characteristics, which are solely disclosed when the product is "exposed to interaction with specifically chosen outside conditions" are not automatically revealed.[1641]

From an economic standpoint, in fast moving industries, with short product life cycles, holders of information do not usually seek patent protection, as the patent term outweighs the expected obsolescence of the secret innovation. In such a context, the lead time conferred by secrecy prior to the reverse engineering of a product is the preferred option to appropriate returns from innovation.[1642]

In sum, it can be concluded that marketing a product does not, as such, disclose any of the inventions and the trade secrets that it embodies, unless they become apparent upon its inspection and analysis. However, at this point a crucial distinction must be made. Under patent law, the mere possibility of accessing the information renders it available for the purposes of assessing its novel character, even if the information is subject to a process of reverse engineering. By contrast, in the case of trade secrets, such an assessment depends on whether third parties (i.e. the relevant circles) have *in fact* examined the marketed product and devised the secret or if the information is accessible (or apparent) with so little labour and intellectual skill that it does not appear reasonable to enforce an obligation of confidence on the acquirer of the product. Consequently, information that is acquired after a process of reverse engineering by a competitor remains eligible for trade secrets protection for as long as it does not become generally known within the industry. As a final note, it is noteworthy that under both legal regimes, the extrinsic characteristics of the product are not immediately disclosed and consequently they are eligible for both patent and trade secrets protection.

1639 G 1/92 [1993] OJ EPO 278.
1640 G 1/92 [1993] OJ EPO 278, 279; Guidelines for Examination in the EPO Part G. Chapter IV. Section 7.2.1.
1641 G 1/92 [1993] OJ EPO 278, 280.
1642 James Pooley 2002 (n 66) § 4.04 34-35.

4. Disclosures on the Internet

To be sure, the Internet has increased the pace with which, and the audience to which, specific information can be disclosed. The publication of trade secrets on the Internet constitutes a prime example of the increasing challenges that stakeholders face in keeping their secrets undisclosed. In such a context, the main issue is whether posting a piece of information on the Internet renders it automatically generally known or readily accessible. This topic has garnered substantial attention in recent years, particularly with the advent of new technologies. The following sections examine the most relevant decisions on this subject in the U.S. (section a), England (section b) and Germany (section c). Finally, some guiding principles that should aid national courts in assessing whether information has entered the public domain are formulated (section d).

a) U.S.

In the U.S., there is no consistent case law on the effects of internet disclosures.[1643] So far, the most relevant cases dealing with trade secret disclosure on the Internet are (i) *Religious Technology Center v. Lerma;*[1644] (ii) *DVD Copy Control Ass'n v. Bunner*[1645] and (iii) *United States v. Genovese*.[1646]

The first case, *Religious Technology Center v. Lerma* concerned a case of misappropriation of trade secrets from the Church of Scientology. The defendant (Mr Lerma), a former member of the Church, posted online information about the Church that he had acquired from a court record. Such information was regarded as a trade secret by the Church, who obtained a temporary restraining order against the defendant.[1647] Notwithstanding

1643 This issue has been explored by several academic articles, the most notable being: Elizabeth A. Rowe 2007 (n 1515) explaining that usually when a trade secret is posted on the internet, the trade secret holder loses its rights on the information and cannot prevent third parties from using it; see further Elizabeth A. Rowe, 'Introducing a Takedown for Trade Secrets on the Internet' [2007] Wisconsin LR 1041arguing that Congress should enact specific takedown legislation vis-à-vis trade secrets; also Victoria A. Cundiff 2009 (n 739) 359 reviewing the measures that the owners of secret information should adopt in order to protect them in the digital environment.

1644 *Religious Technology Center v. Lerma* 908 F.Supp. 1362 (E.D. Va. 1995).

1645 *DVD Copy Control Association Inc. v. Andrew Bunner* 75 P.3d 1 (Cal. 2003).

1646 *United States v. Genovese* 409 F.Supp.2d 253 (S.D.N.Y. 2005).

1647 *Religious Technology Center v. Lerma* 908 F.Supp. 1362, 1364 (E.D. Va. 1995).

this, prior to the issuance of the restraining order, Mr. Lerma had also sent a copy of the posted documents to an investigative reporter working for the Washington Post, Richard Leibi. The reporter ended up publishing an article in the Washington Post based on those materials. As a result, the Church of Scientology brought legal action seeking injunctive relief and damages on the grounds of copyright infringement and trade secret misappropriation against The Washington Post. The first claim on copyright was dismissed by the District Court of Virginia. As regards the trade secret claim, the court noted that the publication of a trade secret online renders it part of the public domain and thus it can no longer be afforded protection.[1648]

Similar arguments were raised by the District Court of California in a subsequent case that also concerned an alleged trade secrets misappropriation brought again by the Curch of Scientology against a former member that posted the Church's writings on an Internet USENET group.[1649] Against this fact pattern the court held that the disputed information was generally known and consequently, it did not merit protection.[1650] Notwithstanding this finding, after several months the Church filed another motion but this time providing consumer surveys.[1651] In its legal reasoning, the District Court changed its previous position and noted that the assessment of secrecy "requires a review of the circumstances surrounding the posting and consideration of the interests of the trade secret owner, the policies favoring competition and the interests, including first amendment rights, (…) of innocent third parties who acquire information of the Internet".[1652] Consequently, the preliminary injunction was issued because under such a test, it was questionable whether the information was public

1648 *Religious Technology Center v. Lerma* 908 F.Supp. 1362, 1368 (E.D. Va. 1995).

1649 *Religious Technology Center v. Netcom On-Line Commc'n Servs., Inc.*, 923 F.Supp. 1231 (N.D. Cal. 1995) (Netcom I); according to footnote 5 of this decision "Usenet news, which is one of the most popular features of the Internet, allows users of systems "subscribing" to the groups to participate by reading and "posting" messages on a particular topic, such as intellectual property rights ("misc. int-property") or table tennis ("rec.sport.table-tennis")".

1650 *Religious Technology Center v. Netcom On-Line Commc'n Servs., Inc.*, 923 F.Supp. 1231, 1256-1257 (N.D. Cal. 1995) (Netcom I).

1651 *Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc.*, 1997 WL 34605244 (N.D. Cal Jan. 6, 1997) (Netcom II).

1652 *Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc.*, 1997 WL 34605244 page 12. (N.D. Cal. Jan. 6, 1997) (Netcom II).

knowledge considering the difficulty in identifying potential competitors.[1653]

The second case, *DVD Copy Control Ass'n v. Bunner*,[1654] concerned the publication of a program on the Internet allowing for the decryption of information stored on DVDs (the so-called "DeSCC" program). The content scrambling system ("CSS") prevented the copying of the content of DVDs and was licensed by the DVD Copy Control Association (a trade association of businesses in the movie industry) to DVD player manufacturers under the condition that they did not reverse engineer the program. Pursuant to the plaintiff, the defendant (Mr Bunner) found the DeSCC program, which allowed for decrypting the CSS secret information, on the Internet, knowing that it had been obtained through reverse engineering in breach of the terms of the licensing agreement, and posted a link to it on his website, invoking the freedom of speech principle enshrined in the first amendment of the U.S. Constitution. On appeal, the Supreme Court of California ruled firstly that if a trade secret existed, the grant of an injunction would not contravene the first amendment and secondly, it added that the plaintiff had failed to provide evidence that the information was still secret at the time that the defendant republished it on his website. It nevertheless noted, that in theory it was possible that the secret nature of the information was not lost, as it had been posted on an "obscure site on the Internet" and detected quickly.[1655] Notwithstanding this, on remand the California Court of Appeal for the Sixth District concluded that the CSS technology was no longer secret and, consequently, held that the grant of a preliminary injunction would negatively affect the freedom of speech principle more than necessary. As a result, the decision to grant the preliminary injunction was reversed.[1656]

1653 Ibid.

1654 *DVD Copy Control Association Inc. v. Andrew Bunner* 75 P.3d 1 (Cal. 2003).

1655 *DVD Copy Control Association Inc. v. Andrew Bunner* 4 Cal. Rptr. 3d 69, 101 (Cal. 2003) noting that that "information posted on an obscure Internet site and detected quickly should not lose trade secret status. This position is consistent with case law holding that minor disclosures of a trade secret followed by a brief delay in withdrawing it from the public domain do not cause the trade secret to be lost".

1656 *DVD Copy Control Association Inc. v. Andrew Bunner*, 10 Cal. Rptr. 3d 185 (Cal. Ct. App. 2004); for a critical overview of first amendment defences in trade secret disclosure cases on the Internet see Pamela Samuelson, 'Principles for Resolving Conflicts Between Trade Secrets and the First Amendment' [2007] 58 Hastings LJ 777, 800-805.

The third case, *United States v. Genovese*, dealt with the publication of parts of Microsoft's source code for two of its operating systems (Windows NT 4.0 and Windows 2000) on the Internet. Following an investigation, the FBI determined that Mr Genovese was offering the source code for sale on his website for 20 USD and, therefore, he was charged for the unlawful downloading and selling of trade secrets in violation of the EEA.[1657] Mr Genovese challenged the indictment, among other reasons, on the basis that firstly, it contravened the first amendment of the U.S. Constitution, which enshrines the freedom of expression principle, and secondly, Microsoft had not adopted reasonable measures to protect it; as the defendant had obtained it from a third party.[1658] In the legal reasoning, the court indicated that the first amendment was indeed applicable to "source code and other types of trade secrets". However, the court concluded that this provision does not afford protection to third parties that intend to economically benefit from another's trade secret by "their unauthorised copying, duplicating, downloading and uploading".[1659] With respect to the reasonable measures claims, it was indicated that Mr Genovese knew that the source code had been unlawfully acquired through the circumvention of technical protection measures and therefore he "could understand" that offering to sell the source code was prohibited by law.

In the light of the foregoing analysis, it is suggested that despite the fact that ultimately secrecy is a question of fact and has to be assessed based on the circumstances of each case,[1660] courts in the U.S. have not adopted a uniform approach to the challenges posed by the Internet in connection with the secrecy requirement[1661] and the potential negative impact of injunctions on freedom of speech.[1662]

b) England

The effects of the disclosure on the Internet of secret information were the object of a decision in 2009 by the High Court of England and Wales in

1657 *United States v Genovese* 409 F.Supp.2d 253, 255 (S.D.N.Y. 2005).
1658 *United States v Genovese* 409 F.Supp.2d 253, 254 (S.D.N.Y. 2005).
1659 *United States v Genovese* 409 F.Supp.2d 253, 256 (S.D.N.Y. 2005).
1660 Roger M. Milgrim 2014 (n 160) § 1.03-1.268.
1661 Melvin F. Jager, *Trade Secrets Law* (Thompsons Reuters 2015) § 3:39.
1662 A number of principles to resolve these types of conflicts are proposed by Pamela Samuelson, 'Principles for Resolving Conflicts Between Trade Secrets and the First Amendment' [2007] 58 Hastings LJ 777, 833-845.

Barclays Bank Plc v Guardian News and Media Ltd.[1663] The case concerned the leakage of nine confidential documents containing information about several transactions carried out by Barclays Bank and their tax treatment. Importantly, the court noted that it was not a case of whistle-blowing because there was no tax evasion involved, only tax avoidance, which is lawful from a legal perspective and essentially consists of optimising tax payments. According to the facts reported in the decision, one of Barclay's employees had shared the secret documents with several members of Parliament and the Guardian News. Subsequently, the newspaper published them on its website in the context of a series of articles on the topic of banking practices and financial institutions. The documents were posted only for four hours before a preliminary injunction was issued compelling Guardian News to take them down. In deciding whether they still retained the necessary confidential nature for a continuation of injunctive relief, Blake J held that in principle information that is generally available on the Internet loses its confidential nature. Notwithstanding this, under this specific fact-pattern he concluded that "very limited dissemination and only partial dissemination perhaps in some remote or expert site that is not generally available to the public without a great deal of effort, may not result in such a loss of confidentiality".[1664] The deciding factor was thus that the documents were available online for a very limited period of time, and as a result retained their confidential nature.

c) Germany

At first glance, German case law and academia seem to indicate that the disclosure of information on the Internet deprives it of its secret nature.[1665] Indeed, in a case concerning the misappropriation of the Clinical Expert Report of a pharmaceutical product (Movicol) by a former employee who went on to work for a competitor, the Federal Supreme Court ruled that information in the Clinical Expert Report may be deprived of its secret nature if at the time of the disclosure the information was available on the Internet in German or in international specialised publications.[1666]

1663 *Barclays Bank Plc v Guardian News and Media Ltd* [2009] EWHC 591 (QB).
1664 *Barclays Bank Plc v Guardian News and Media Ltd* [2009] EWHC 591 (QB) 22.
1665 *Ohly*/Sosnitza (n 813) § 17 Rdn 9.
1666 BGH GRUR 2012, 1048 Rdn 24 –*Movicol* (Zuassungsantrag).

By contrast, in 2016 the Higher Regional Court of Kalsruhe ruled that the code to unlock SIM cards constituted a protectable trade secret under German law, even though the codes were available on the Internet through special unlocking software, which was made available without authorisation by the defendant upon payment of a fee. In such a context, the court concluded that the technical protection measures implemented by the plaintiff, as well as the difficulty and cost involved in obtaining the codes preserved the undisclosed nature of the information and hence it was protectable as a trade secret.[1667]

d) Guiding principles

As is apparent from the comparative analysis conducted in the previous sections, the general principle is that once information is posted on the Internet, it becomes generally known. However, in certain cases, courts in the three jurisdictions studied have ruled that the secret nature of information subsisted, despite the fact that it had been made available online.

In this context, Rowe suggests a "sequential preservation model", whereby in exceptional circumstances the publication of a trade secret on the Internet should not be deemed secrecy-destroying. According to the author, the three parameters to be weighed in are: (i) the time that the secret was available on the Internet, together with the time it took the holder to take legal action; (ii) the extent of the disclosure; and (iii) the recipient's reason to know that the information was a trade secret.[1668]

The starting point of the analytical framework proposed by Rowe should be whether at the time of the unauthorised online disclosure, the information complied with the statutory requirements of protection, i.e., whether (i) it was secret, (ii) had commercial value as a result of its secret nature, and (iii) was subject to reasonable steps under the circumstances to maintain its secret status.[1669] Clearly, if the information did not meet ex ante any of these requirements, the disclosure should not be deemed unlawful, as the object of protection had ceased to exist.

Next, the first factor proposed by Rowe takes into consideration the amount of time that the information was available online and the measures that the trade secret holder adopted upon finding out about the dis-

1667 OLG Karlsruhe MMR 2016, 562.
1668 Elizabeth A. Rowe 2007 (n 1515) 30-38.
1669 Elizabeth A. Rowe 2007 (n 1515) 33-34.

closure.[1670] According to the author, the risks associated with the dissemination of information on the Internet impose a duty of monitoring on trade secrets holders and, in correlation, a duty to take action as soon as a disclosure is identified.[1671] Such measures include launching legal actions, applying for a preliminary injunction, sending a cease and desist letter or requesting the owner of the website to take down the secret information.[1672] Reacting promptly is crucial to ensure that the object of protection is not lost. This is also in line with Recital 26 TSD, where it is noted that it "is essential to provide for fast, effective and accessible provisional measures for the immediate termination of the unlawful acquisition, use or disclosure of a trade secret", in view of the devastating effects that such conduct may have on the trade secret holder as a result of the loss of secrecy. In this context, Rowe convincingly concludes that it is unlikely that information that has been available online for more than forty-eight hours can be considered to retain its secret nature, even though this will ultimately depend on the specific circumstances of the case.[1673] Indeed, in *Barclays Bank Plc v Guardian News and Media Ltd* injunctive relief was granted on the basis that the information had only been available for four hours.[1674]

The second factor evaluates the extent of the disclosure in order to assess whether the information has become "generally known or knowable".[1675] It primarily looks into the specific characteristics of the website and the extent of the actual dissemination. In effect, disclosures on obscure websites are more likely to be non-secrecy destroying than disclosures on high-traffic websites. In addition, courts should also take into consideration whether the access was limited, for instance, restricted to members with an account. This is crucial to assess whether the relevant circles may have had access to the information concerned and as a result, may have acquired active knowledge of said information. Furthermore, due account should be paid to the amount of information published. Partial disclosures only affect the nature of the specific information disclosed.[1676]

1670 Elizabeth A. Rowe 2007 (n 1515) 32.
1671 Elizabeth A. Rowe 2007 (n 1515) 32-33; similar views are expressed by the EU legislator in Recital 23 TSD with respect to the limitation period.
1672 Elizabeth A. Rowe 2007 (n 1515) 33
1673 Elizabeth A. Rowe 2007 (n 1515) 33.
1674 *Barclays Bank Plc v Guardian News and Media Ltd* [2009] EWHC 591 (QB) [32].
1675 Elizabeth A. Rowe 2007 (n 1515) 33.
1676 Lionel Bently and Brad Sherman 2014 (n 125) 1148.

The third factor is the most controversial one, as it enquires into the defendant's "state of mind".[1677] According to Rowe, if the information is posted on the Internet by a misappropriator or a third party that had reason to know that the information had been misappropriated, liability should arise.[1678] A similar approach has been adopted by the EU legislator in the TSD. According to Article 4(3) TSD, the disclosure of a trade secret acquired unlawfully or in breach of a secrecy obligation or any other duty not to disclose the information triggers liability. Consequently, if the information is posted on a website, for instance, by a party in breach of an obligation of confidence, the said party will be deemed liable for the unauthorised disclosure of a trade secret. Furthermore, pursuant to Article 4(4) TSD, if the party that disseminates the information online knew or should have known under the circumstances that the information was obtained from an illicit source, such disclosure should be considered illicit and consequently trigger liability. Notwithstanding this, it seems unsound to enjoin bona fide third parties that acquire information by merely checking a website from using or disclosing the said information without knowledge or reason to know the unauthorised origin of the information. In such a context, if as a result of its wide dissemination the trade secret holder loses control over the subsequent use and disclosure of the information and it enters the public domain, the secret as such ceases to exist.[1679]

Likewise, in her analytical framework, Rowe purports that infringers should not be able to counterclaim that upon publication the obligation ceases to exists. Infringers should be liable because at the time of the disclosure the information complied with the statutory requirements for protection.[1680] This view is in line with Article 13(1) paragraph 2 TSD, which provides that when an injunction is ordered with a time limit, its "duration shall be sufficient to eliminate any commercial or economic advantage that the infringer could have derived from the unlawful acquisition, use or disclosure of the trade secret". Similarly, the TSD provides that preliminary and precautionary measures, as well as injunctions and corrective measures shall be revoked if the information no longer meets the requirements of protection "for reasons that cannot be attributed to the respon-

1677 Elizabeth A. Rowe 2007 (n 1515) 34.
1678 Elizabeth A. Rowe 2007 (n 1515) 36-37.
1679 Elizabeth A. Rowe 2007 (n 1515) 36.
1680 Elizabeth A. Rowe 2007 (n 1515) 35-37; Roger M. Milgrim 2014 (n 160) § 17.03 15

dent".[1681] Consequently, the fact that the information has become generally known does not exonerate of liability the infringer who publishes the information on the Internet with knowledge (or being gross negligent) of the illicit source of the information. Yet, trade secrets are not enforceable against third parties that have acquired them lawfully.

In this context, Rowe suggests that failure to act promptly upon being notified of the infringing nature of the online publication (step 1 of the sequential model) should also trigger liability.[1682] This also seems to be the prevailing legal view under the harmonised EU legal framework, where liability for bona fide third parties arises upon notification of the confidential nature of the information.[1683] This in turn raises questions regarding the potential liability of intermediaries, such as online platforms, that are used as the means to disclose the information and that do not take it down upon being notified by the trade secret holder of its infringing nature. Ultimately, the intersection between the hosting safe harbour established in Article 14(1) of the Directive on electronic commerce and the TSD will have to be subject to judicial interpretation by the CJEU.[1684]

In the light of the above, the better view, it is submitted, is that the assessment of whether information that is published on an Internet webpage loses its secret nature should be conducted on a case-by-case basis, taking into consideration the likelihood that members of the relevant public have in fact accessed the information. Crucial factors include the length of time during which the information was posted online and the measures adopted upon discovery of the publication.[1685] Courts should also take into consideration the website traffic and the extent of the disclosure (whether it is partial or total) in order to assess whether it has become generally known among the relevant circles.[1686] However, these factors should be viewed as mere guidelines with no normative value. Indeed, affording normative val-

1681 Recital 27 TSD.
1682 Elizabeth A. Rowe 2007 (n 1515) 36.
1683 See Article 4(4) TSD and 13(3) TSD and Recital 29.
1684 As analysed in chapter 3 § 5 C) III. 2. c).
1685 Similar views are expressed by Roger M. Milgrim 2014 (n 160) § 17.03 15 who notes that "publication on the Internet does not necessarily terminate trade secrets status; inasmuch as trade secret statues is an intense question of fact (…) the factual question must be answered as to whether as a matter of fact the matter is readily available or ascertainable".
1686 Pamela Samuelson, 'Reverse Engineering Under Siege' [2002] 45 Commmunications of the Association Computing Machinery 15, text acomanying footnote 7.

ue to such a test would disregard the essentially factual nature of secrecy. On the contrary, considering every single publication on the Internet as secrecy destroying would amount to an absolute test of secrecy, ignoring the principle of inaccessibility that is supported in all of the jurisdictions studied and disregarding whether the trade secret holder has control over the subsequent use and disclosure of the information concerned. As regards the third factor propounded by Rowe, it should be noted that the liability of third parties is in fact regulated under Article 4(4) TSD following a gross negligence standard, in line with footnote 10 of Article 39 TRIPs. Therefore, it seems unreasonable to enforce generally known information against third parties that consult a webpage without knowledge or reason to know the illicit source of the information. To hold otherwise would upset the balance between formal IPRs and non-formal information.

5. Limited content: combination secrets

Frequently, trade secrets consist of a number of elements, some of which (if not all) are part of the public domain. However, this does not necessarily preclude the application of trade secrets liability rules in the case of misappropriation. Courts in the US,[1687] England[1688] and Germany[1689] have acknowledged the existence of so-called "combination secrets", which have been defined as "a multi-element claim that, when valid, ties non-secret items of information together in a unique manner to form a trade secret".[1690] This concept presents clear parallelisms with the definition of a database provided in Article 1(2) of the Database Directive, which refers to them as the "collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means". Hence, combination secrets can constitute the object of a database protected both under copyright and the sui generis right, provided that the requirements of protection under both regimes are met. However, the database sui generis legal regime also foresees that the lawful user shall be entitled to extract "insubstantial parts" of its contents,

1687 *Merck v. Smithkline Beecham Pharm Co*., No. C.A. 15443-NC (Del. Ch 1999).
1688 *Under Water Welders & Repairers Ltd v Street and Longthorne* [1968] RPC 498 (QB), 506-507.
1689 BGH GRUR 1966, 576 – *Zimcofot.*
1690 Charles Tait Graves and Brian D. Range, 'Identification of Trade Secret Claims in Litigation: Solutions for a Ubiquitous Dispute' [2006] 5 New J of Technology IP 68, 77.

which may compromise the secret nature of the information and consequently, its elegibility for protection as a trade secret.[1691]

The protection of combination secrets is in line with Article 39(2)(a) TRIPs, which stipulates that information is secret if it "is not, as a *body or in the precise configuration and assembly of its components*, generally known among or readily accessible". Thus, following the wording of TRIPs, which has also been incorporated into Article 2(1)(a) TSD, the assembly of individually known components can also constitute the object of a trade secret.[1692]

In the following sections, several cases concerning combination secrets in the U.S. (section a), England (section b) and Germany (section c) are examined. Next, drawing from such an analysis, a number of interpretative principles regarding the protectability of combination secrets are formulated, with the purpose of finding an equilibrium with the public domain boundaries in the interests of competition, innovation and employee mobility (section d).

1691 Chapter 1 § 3 A) IV. 1.

1692 Gerald Reger 1999 (n 553) 362; surprisingly, the definition set out in § 2(1) of the proposed German Trade Secrets Act ("Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/680 im Strafverfahren sowie zur Anpassung datenschutzrechtlicher Bestimmungen an die Verordnung (EU) 2016/679)") is more restrictive than the one followed by Article 2(1)(a) TSD. The German legislator has stipulated that information is secret when it is "neither as a body nor 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". According to the German definition, to merit protection, information must not be generally known as a body and in its individual components simultaneously. Consequently, both requirements are cumulative under German law, and not alternative, as laid down in the TSD and TRIPs. As a result of such a narrow definition, the possibility of protecting combination secrets in Germany may be excluded in the future, because to be secret information needs to be unknown as a whole and in its individual elements, irrespective of whether the aggregation of individual components, such as data, results in a new and unknown entity; see further Luc Desaunettes, Reto M. Hilty, Roland Knaak, Annette Kur, 'Stellungnahme zum Referentenentwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/943 zum Schutz von Geschäftsgeheimnissen vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung vom 17. April 2018' (2018), para 7 and 8 <https://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/Stellungnahme_zum_Referentenentwurf_eines_Gesetzes_zur_Umsetzung_der_Richtlinie__EU__2016_943.pdf> accessed 15 September 2018.

a) U.S.

The origin of the protection of combination secrets in the U.S. can be traced back to the end of the XIX century. It emerged as a result of the intersection between labour law and trade secrets protection, after several courts refused to grant injunctions against former employees on the basis that the information for which protection was sought was in fact part of the public domain.[1693] In turn, plaintiffs usually counter-claimed that the combination of known elements deserved protection because of the new results and utility produced by the specific combination of such elements.[1694] Since the end of the XIX century, the concept of combination secrets has been incorporated into the four main sources of trade secrets law in the U.S and has given rise to a rich body of case law: the Restatement (First) of Torts;[1695] the Uniform Trade Secrets Act;[1696] the Restatement (Third) of Unfair Competition[1697] and more recently the DTSA of 2016.[1698] Most frequently, when deciding on the protection of combination secrets, courts have been confronted with the issue of deciding whether the alleged combination is common among industry members and consequently should be deemed "generally known" or instead deviates sufficiently from such practices to merit protection as a discrete entity.[1699]

1693 See Charles Tait Graves and Alexander Macgillivray 2004 (n 699) 267 with further references.

1694 *Eastman Co. v. Reichenbach*, 20 N.Y.S. 110 (1892).

1695 See Restatement (First) of Torts § 757 (Am. Law Inst. 1939) comment g, where it is noted that trade secrets may consist of a "compilation". Notably, the comment does not provide further guidance regarding the circumstances under which said "compilations" may be protected.

1696 UTSA § 1(4) defining trade secret as a "formula, pattern, *compilation*, program, device, method, technique or process" (emphasis added).

1697 Restatement (Third) of Unfair Competition §39 (Am. Law Inst. 1995) comment f: "It is the secrecy of the claimed trade secret as a whole that is determinative. The fact that some or all of the components of the trade secret are well-known does not preclude protection for a secret combination, *compilation*, or integration of the individual elements"(emphasis added).

1698 18 U.S.C. § 1839 (3) defining the term trade secrets as: "all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, *compilations*, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, *compiled*, or memorialized physically, electronically, graphically, photographically, or in writing (…)" 1(emphasis added).

1699 Charles Tait Graves and Alexander Macgillivray 2004 (n 699) 271-272.

For instance, in 2002 the Supreme Court of Arkansas ruled in favour of Wal-Mart Inc. in a case that involved the alleged misappropriation of a trade secret by the U.S. multinational retail corporation.[1700] In 1992 the legal representative of the plaintiff ("The P.O. Market Inc.") approached a manager of a Wal-Mart store regarding an idea to execute bulk credit transactions, which essentially consisted of transferring the risk of non-payment of wholesale orders to the plaintiff, an intermediate company that would place the orders to Wal-Mart Inc. on behalf of the customers.[1701] In 1992, a number of meetings between the representatives of The P.O. Market Inc. and Wal-Mart Inc. took place under strict confidentiality but eventually the negotiations broke off.[1702] In 1993 the Wall Street Journal published an article in which it described a new purchasing programme set up by Wal-Mart Inc., by virtue of which bulk purchasers were allowed to buy goods on credit.[1703] Thereafter, The P.O. Market Inc. brought legal action against Wal-Mart Inc. for trade secrets misappropriation. The plaintiffs prevailed in the first instance, but upon appeal, the Supreme Court of Arkansas held that the alleged trade secret was not a unique concept, as it was merely "a variation of other economic models" already in the public domain. In its legal reasoning the Court noted that "any person reasonably well vested in the economics of wholesaling and credit purchasing could have put together the (...) concept".[1704]

A similar reasoning was applied by the Court of Appeals of the Federal Circuit in *Julie Research Laboratories, Inc. v Select Photographic Engineering Inc.*,[1705] where it was ruled that the retouching imaging system developed by the plaintiff consisted of a combination of twelve system design choices. These were "either obvious, widely known, easy for others to discover legitimately or disclosed in the sales literature of the plaintiff or other manufacturers".[1706] Consequently, trade secrets protection was denied.

1700 *Wal-Mart Stores, Inc. v. The P.O. Market Inc.*, 66 S.W.3d 620 (Ark. 2002).
1701 *Wal-Mart Stores, Inc. v. The P.O. Market Inc.*, 66 S.W.3d 620, 622 (Ark. 2002).
1702 *Wal-Mart Stores, Inc. v. The P.O. Market Inc.*, 66 S.W.3d 620, 623-624 (Ark. 2002).
1703 *Wal-Mart Stores, Inc. v. The P.O. Market Inc.*, 66 S.W.3d 620, 626 (Ark. 2002).
1704 *Wal-Mart Stores, Inc. v. The P.O. Market Inc.*, 66 S.W.3d 620, 634 (Ark. 2002).
1705 *Julie Research Laboratories, Inc. v. Select Photographic Engineering Inc.*, 998 F.2d 65 (2d Circ. 1993).
1706 *Julie Research Laboratories, Inc. v. Select Photographic Engineering Inc.*, 998 F.2d 65, 67 (2d Circ. 1993).

By contrast, in *Merck v. Smithkline Beecham Pharm Co*,[1707] the Court of Chancery of Delaware ruled that the commercial process for the production of a varicella vaccine developed by the Japanese pharmaceutical company, Biken, and subsequently licensed to Merck, constituted a trade secret, despite the fact that certain aspects of the laboratory process for the production of the varicella vaccine could be found in a publication from the 1970s.[1708] Against this background, the court clearly distinguished between the laboratory process described in the said publication and the commercial production process misappropriated by the defendant, because the former did not solve some of the practical problems that the manufacturers encountered in the production phase.[1709]

Likewise, in *Penalty Kick Management, Ltd. v. Coca-Cola Co.*[1710] the protection of combination secrets was affirmed. The facts of the case are as follows: in 1995 the Chief Executive of Penalty Kick Management ("the Plaintiff") developed a "beverage label marketing and production process known as Magic Windows".[1711] It essentially consisted of inserting a message on the inside of the label of the bottle that had to be read through a coloured filter once the container was emptied.[1712] In the same year, two executives of the Plaintiff met with the representatives of The Coca-Cola Co., Atlanta, GA ("the Defendant") in order to show them the marketing and production process for the new label developed by their company. During the course of the meeting, the representatives of the Plaintiff mentioned that they had filed a patent application for the Magic Windows and that everything discussed in the meeting was to be kept confidential. Sometime later, in 1996, the parties executed an NDA and started negotiating the content of the licensing agreement. However, before it was executed, the defendant examined some of the published patent applications and concluded that the Magic Window concept was in fact in the public do-

1707 *Merck v. Smithkline Beecham Pharm Co*., No. C.A. 15443-NC (Del. Ch 1999).
1708 *Merck v. Smithkline Beecham Pharm Co*., No. C.A. 15443-NC (Del. Ch 1999).
1709 *Merck v. Smithkline Beecham Pharm Co*., No. C.A. 15443-NC 18 (Del. Ch 1999); this decision was subsequently upheld by the Supreme Court of Delaware in *Smithkline Beecham Pharmaceuticals Co. v. Merck & Co., Inc.,* 766 A.2d 442 (Del. 2000).
1710 *Penalty Kick Management, Ltd. v. Coca-Cola Co,* 318 F. 3d 1284 (11th Cir. 2003).
1711 *Penalty Kick Management, Ltd. v. Coca-Cola Co,* 318 F. 3d 1284, 1286-1287 (11th Cir. 2003).
1712 *Penalty Kick Management, Ltd. v. Coca-Cola Co,* 318 F. 3d 1284, 1286-1287 (11th Cir. 2003).

main.[1713] Hence, the defendant asked one of its label printer contractors to develop a bottle with a label, which was very similar to the Magic Windows.[1714] When the Plaintiff found out, he brought legal action against the defendant for trade secrets misappropriation and breach of the NDA. In turn, the defendant counter-claimed that the information revealed on the Magic Windows was not a trade secret and that the terms of the NDA had not been infringed. In its legal reasoning, the District Court for the Northern District of Georgia started by noting that, "the fact that some or all the elements of the trade secret are well-known does not preclude protection for trade secrets combination, compilation, or integration of the individual elements".[1715] According to the Court, a "unique combination of that information" may be eligible for protection, provided that it "adds value to the information".[1716] In view of this, the Court held that the Magic Windows constituted a trade secret because many aspects were unique if compared to the existing prior art. However, the court ruled that the Plaintiff had failed to prove that the label used by the Defendant "substantially derived" from the Plaintiff's label and came to the conclusion that the information used by the Defendant had been independently generated by him.[1717]

In sum, it appears that courts in the U.S. seem inclined to afford protection to combination secrets when the unique compilation of known information provides a solution to an unsolved problem or, more generally, when it confers additional value to the information viewed as a whole. By contrast, the mere combination of known elements should not merit protection if no intellectual skill is necessary to put it together. To hold otherwise would entail the privatisation of information already in the public domain.

1713 *Penalty Kick Management, Ltd. v. Coca-Cola Co,* 318 F. 3d 1284, 1288 (11th Cir. 2003).

1714 *Penalty Kick Management, Ltd. v. Coca-Cola Co,* 318 F. 3d 1284, 1288 (11th Cir. 2003).

1715 *Penalty Kick Management, Ltd. v. Coca-Cola Co,* 318 F. 3d 1284, 1291 (11th Cir. 2003).

1716 *Penalty Kick Management, Ltd. v. Coca-Cola Co,* 318 F. 3d 1284, 1291 (11th Cir. 2003).

1717 *Penalty Kick Management, Ltd. v. Coca-Cola Co,* 318 F. 3d 1284, 1295-1298 (11th Cir. 2003).

b) England

The possibility of protecting combination secrets has been established in a number of landmark decisions of the English jurisdiction, such as *Coco v AN Clark Engineers Ltd*,[1718] in which Megarry J noted that, "something that has been constructed from materials in the public domain must possess the necessary quality of confidentiality".[1719] This statement clarifies that the test of inaccessibility is to be applied with respect to the information "considered as a discrete entity, independent of its component parts".[1720]

This principle was most famously acknowledged by Hawkings J in *Robb v Green*,[1721] a case concerning the unauthorised copying of the order book of the plaintiff by one of his former employees during the course of the employment relationship. The employee subsequently set up a competing business and used the copies of the book to target orders to the customers. With respect to the existence of a breach of confidence, the defendant argued that the information in the order book was publicly available in other sources.[1722] In this regard, it was held that:

> The names of all the customers are collected together in the order-book in a manner not to be found in any other book or paper to which the defendant had access. To him, therefore, the possession of a copy of the order-book would be peculiarly valuable. He would be saved the expense and delay of searches, such as would be necessary to enable him to compile such a list for himself (…) By making a copy of the order-book defendant was able to canvass at once each of his master's customers without trouble or expense.[1723]

As is apparent from the above, combination secrets will only be deemed secret if a certain degree of skill and labour is necessary to bring them together.[1724]

Such a principle was subsequently restated by Laddie J in *Ocular Sciences Ltd v Aspect Vision Care Ltd*,[1725] a case that broadly speaking involved two actions. The first concerned an alleged breach of confidence, a breach of

---

1718 *Coco v AN Clark Engineers Ltd* [1969] RPC 41 (Ch).
1719 *Coco v AN Clark Engineers Ltd* [1969] RPC 41 (Ch), 47.
1720 Tanya Aplin and others 2012 (n 22) para 5.16.
1721 *Robb v Green* [1895] 2 QB 1 (QB).
1722 *Robb v Green* [1895] 2 QB 1 (QB), 18-19.
1723 *Robb v Green* [1895] 2 QB 1 (QB), 18-19.
1724 John Hull 1998 (1016) para 3.28.
1725 *Ocular Sciences Ltd v Aspect Vision Care Ltd* [1997] RPC 289 (Pat).

contract and a breach of fiduciary duty, as well as a design and copyright infringement claim brought by two companies that designed, manufactured and sold contact lenses against their former employees. The second dealt with a patent infringement claim. Of particular interest for the purposes of the current analysis is that in deciding whether a booklet with all of the specifications of the lenses manufactured by the plaintiff was confidential, Laddie J questioned whether the "mere mechanical collection of data which is in public domain" could be deemed confidential. He further noted that to be treated as confidential, "there must be some product of the human brain".[1726] Such a distinction is a crucial one, as it indicates that effort, time and labour are not sufficient to confer the necessary quality of confidence upon information that is in the public domain.[1727] Thus, it appears that some intellectual skill is essential to regard the compilation of information as protectable.[1728] However, in this context, intellectual skill is to be differentiated from other IPRs normative standards such as novelty or inventive step. It is understood to refer to the trial and error process that gives rise to a unique combination of publicly available items.[1729]

c) Germany

German commentators and case law have developed a so-called "mosaic approach" to conceptualise the protection of combination secrets, by virtue of which a combination of known elements may only constitute a trade secret if it is not known as such and derives additional value from becoming a new entity.[1730] In this scenario, it is regarded that the object of protection is the unknown combination of already known elements,[1731] which is justified on the basis that the compilation of information in a systematic manner can be very costly and time consuming. Indeed, it is the effort put into collecting and systematising the data that merits protection.[1732]

1726 *Ocular Sciences Ltd v Aspect Vision Care Ltd* [1997] RPC 289 (Ch), 375.
1727 Tanya Aplin and others 2012 (n 22) para 5.16.
1728 Tanya Aplin and others 2012 (n 22) para 5.20.
1729 John Hull 1998 (1016) para 3.28 and para 3.35.
1730 Björn H. Kalbfus 2011 (n 1300) para 138; Peter Finger, 'Die Offenkundigkeit des mitgeteilten Fachwissens bei Know-how-Verträgen' [1970] GRUR 3, 7; BGH GRUR 1966, 576 – *Zimcofot.*
1731 Charles Tait Graves and Alexander Macgillivray 2004 (n 699) 270.
1732 Björn H. Kalbfus 2011 (n 1300) para 138.

This principle was clearly stated by the Federal Supreme Court in a decision in 2006 (*Kundendatenprogramm*),[1733] which concerned the misappropriation of a client list by one of the former employees of the plaintiff who went on to work for one of its competitors (both PBC panels' manufacturers). As regards the secret nature of the information, the Federal Supreme Court held that:

> as long as a customer list does not consist merely of the list of addresses that can be easily found in public sources, it can be protected as a trade secret despite a low price for which such customer list was obtained. (…) Trade secrets do not necessarily feature as such property value (…). It derives from the nature of the customer lists that their value lies rather in the fact that they are not accessible to the competitors.[1734]

Consequently, the list, as a discrete entity, should be deemed secret if the names and additional data are gathered and assembled in a manner that would not otherwise be available to competitors.

In line with this argument, in Germany, case law and commentators have asserted that under certain circumstances the use of known information for an unknown end may merit trade secrets protection. This mostly takes place when an undertaking secretly uses a known process to achieve a result that is not known to its competitors,[1735] in a similar manner to the second medical indication exception under patent law set out in Article 54(5) EPC.[1736] However, to merit protection, it is crucial that the competitors are not aware of the use of the trade secret for that specific purpose.[1737] The object of protection is not that the company is using such a process, but rather that it can be applied to achieve an unknown result.[1738]

This was famously held by the Federal Supreme Court in a decision dated 15 March 1955 concerning a secret process to manufacture wax paste for furniture. Since 1931, the plaintiff had been producing wax paste for furniture according to a process that he had developed and kept undis-

---

1733 BGH GRUR 2006, 1044 – *Kundendatenprogramm.*

1734 BGH GRUR2006, 1044, Rdn 19 – *Kundendatenprogramm* translation by Gintare Surblyte 2016 (n 281) 12.

1735 Björn H. Kalbfus 2011 (n 1300) para 137.

1736 Article 54(5) EPC.

1737 Rudolf Kraßer 1970 (n 831) 590.

1738 Björn Joachim, Mary-Rose McGuire, Jens Künzel and Nils Weber, 'Der Schutz von Geschäftsgeheimnissen durch Rechte des Geistigen Eigentums und durch das Recht des unlauteren Wettbewerbs' [2010] GRUR Int 829, 829.

closed.[1739] In 1946 he hired one of the defendants to whom he revealed the secret manufacturing process. Subsequently, in 1948 the defendant terminated his employment relationship and started working for another company that manufactured and distributed chemical products. In February 1949, the plaintiff brought legal action based on § 17 UWG against the former employee and the new employer seeking to enjoin the further production of wax paste for furniture according to the process that he had developed.[1740] In May 1949 the parties reached a licensing agreement by virtue of which the plaintiff was entitled to receive a percentage of the turnover of the sales of the wax paste (between 5% and 6%). However, sometime later, the competitor introduced modifications to the formula and stopped paying the agreed fees to the plaintiff, which in turn led to further legal actions. Against this fact-pattern, the defendant provided evidence that the process was well-known and, consequently, the object of the licensing agreement had ceased to exist. In this context, the Federal Supreme Court ruled that a secret process could be known and still qualify for protection, provided that the use of the secret by the company to achieve a specific result was kept undisclosed.[1741] Ultimately, the appeal was dismissed because the variations introduced by the defendants were regarded as minor and, therefore, the validity of the licensing agreement was affirmed. The Federal Supreme Court later restated this argument in subsequent decisions, such as in *Kieselsäure*.[1742]

While German case law and commentators seem eager to support this principle,[1743] it is submitted here that courts should be cautious in its application, which should be limited to exceptional circumstances where the use of a known-process for an unknown use is not inferable from the state of the art and where companies have achieved a great competitive advantage because of its application. Indeed, in *Möbelpaste,* the process to manufacture the furniture wax paste was not objectively new, but was new for the competitor, who had no technical background. In such a context, it should be borne in mind that with time trade secrets erode as competitors independently generate the secret information, which in turn with time may enter the public domain. Hence, the use of a known process for an unknown result shall only be deemed secret to the extent that substantial

1739 BGH GRUR 1955, 424 – *Möbelpaste.*
1740 BGH GRUR 1955, 424, 424 – *Möbelpaste.*
1741 BGH GRUR 1955, 424, 425 – *Möbelpaste*
1742 BGH GRUR 1963, 207, 2011 – *Kieselsäure*.
1743 Björn H. Kalbfus 2011 (n 1300) para 137.

intellectual investment (a process of trial and error) by a circle of experts is necessary to link the process with the unknown result.

In the following section, a number of principles regarding the protection of combination secrets are suggested in order to avoid the privatisation of information that is in fact part of the public domain.

d) Guiding principles

The protection of combination secrets and its implications for competition, innovation and employee mobility have been largely understudied by legal academia, yet the risks posed by such a tendency should not be overlooked.[1744] If courts affirm the protection of trade secrets that are already in the public domain by issuing injunctions against former employees or by enforcing non-competition agreements, the economic and social benefits associated with information dissemination and re-use may potentially be hindered.[1745] Furthermore, some commentators in England and the U.S. have expressed concerns about the fact that combination secrets claims may be used by plaintiffs in abusive litigation to avoid defining the specific subject matter covered by the secret information.[1746] Indeed, the comparative analysis conducted in the previous sections underscores that courts do not always evaluate the broader consequences for the public domain of confirming or denying such protection. In addition, a loose interpretation of such a principle is not in line with the TSD and the TTBER. The former notes that the injunctions and corrective measures adopted by virtue of Article 12 shall be revoked if the information no longer meets the requirements for protection (of which secrecy is one).[1747] In the same vein, the Guidelines on the application of the TTBER note that, "in the case of know-how the block exemption applies as long as the licensed know-how remains secret, except where the know-how becomes publicly known as a result of action by the licensee, in which case the exemption applies for the

1744 Charles Tait Graves and Alexander Macgillivray 2004 (n 699) 274.
1745 Charles Tait Graves and Alexander Macgillivray 2004 (n 699) 274.
1746 Charles Tait Graves and Brian D. Range, 'Identification of Trade Secret Claims in Litigation: Solutions for a Ubiquitous Dispute' [2006] 5 New JTechnology and IP 68, 77 -78; Roger M. Toulson and Charles M. Phipps 2012 (n 326) paras 3-086 -3-088.
1747 Article 13(2) TSD.

duration of the agreement".[1748] The general rule should be that once the secret nature of the information is lost, protection should also cease. Consequently, it is submitted that courts should be cautious when affording protection to combination secrets.

Drawing from Graves' scheme,[1749] this section proposes a number of interpretative principles that courts in the EU should take into consideration in the assessment of whether the combination of known elements (or known elements tied together with some unknown elements) merits protection as a discrete entity under Article 2(1) TSD. These principles intend to provide an analytical framework to avoid conferring exclusivity over information that is in fact already part of the public domain.

The first principle to be taken into consideration is whether "there is a functional interrelationship between the elements in the claimed combination secret".[1750] Graves suggests that courts should examine on a case-by-case basis whether the elements that constitute the trade secret are functionally interrelated in a machine, process or formula.[1751] This essentially means that the different elements have to be integrated following a "unified process that interoperates to form a unit", where all of the steps are necessary to achieve the end result.[1752] This first principle is crucial to ensure that the combination secret constitutes a discrete entity by requiring that it results from the application of a unified process. For instance, in chemical formulas, such as perfume compositions, the ingredients are frequently individually known, yet it is the interaction of the individual components that leads to a unique odour. Similarly, the value of a customer list lies in the systematic and methodical arrangement of its contents collected over time.[1753] Thus, the application of this principle would avoid rulings like *Tan-Line Sun Studios, Inc. v. Bradely*,[1754] where the methodology of the plaintiff, a tanning studio franchise, was considered protectable as a combination secret, even though it included methods of employee re-

1748 Commission, 'Guidelines on the application of Article 101 of the Treaty on the Functioning of the European Union to technology transfer agreements' [2014] OJ C89/3, para 67.

1749 Charles Tait Graves and Alexander Macgillivray 2004 (n 699) 274.

1750 Charles Tait Graves and Alexander Macgillivray 2004 (n 699) 276.

1751 Charles Tait Graves and Alexander Macgillivray 2004 (n 699) 277.

1752 Charles Tait Graves and Alexander Macgillivray 2004 (n 699) 277 citing among other U.S. cases *Saforo & Assoc., Inc. v. Porocel Corp.*, 991 S.W.2d 117, 121 (Ark.1999), where combination secrets where described as a "unified process".

1753 As noted by the BGH GRUR 2006, 1044 – *Kundendatenprogramm.*

1754 *Tan-Line Studios Inc. v. Bradley,* 1 U.S.P.Q.2d 2032 (E.D. Pa. 1986).

cruitment and training, studio layout and cash control, as well as marketing strategies, all of which were known to its competitors.[1755] In sum, it is submitted that the application of this principle would prevent the granting of protection to individual elements in the public domain that are used simultaneously by the plaintiff, i.e. the privatising of generally known information.

The second principle indicates that the combination secret as a discrete entity should have more value than the individual elements considered in isolation.[1756] This principle appears both in English case law (*Robb v Green*)[1757] and German decisions (*Kundendatenprogramm*).[1758] It essentially submits that the secret combination of known elements must be more valuable than its individual components. In addition, the value of the combination secret should be assessed against the other available alternatives, in line with the third principle proposed.[1759]

The third principle suggested by Graves enquires into whether the combination was *obvious*.[1760] At first glance, such a statement seems to contravene the general notion that trade secrets need not be novel, inventive or original. Indeed, as examined below, novelty or inventiveness in the sense of patent law are not required, nor is copyright originality.[1761] Consequently, it is submitted that the better wording, following the prevailing case law in England, is that known information should only merit protection if the combination results from the investment of "*intellectual skill*", i.e. it is a product of the mind of the trade secret holder. Indeed, information that can be automatically obtained (i.e. without the investment of intellectual skill) will rarely be regarded as secret, as it will mostly be considered "readily accessible".

Whether the plaintiffYet again, the problem lies in defining the necessary investment of "intellectual skill" from a qualitative and quantitative perspective. It is proposed here that such a standard is assessed against the existing alternatives used by the relevant circles. From a quantitative perspective, if in view of the existing alternatives the combination of known elements could be carried out automatically without further intellectual contribution from the holder that claims ownership (i.e. without undergo-

---

1755 *Tan-Line Studios Inc. v. Bradley,* 1 U.S.P.Q.2d 2032, para 7 (E.D. Pa. 1986).
1756 Charles Tait Graves and Alexander Macgillivray 2004 (n 699) 279-281.
1757 *Robb v Green* [1895] 2 QB 1 (QB), 17-18.
1758 BGH GRUR 2006, 1044 – *Kundendatenprogramm.*
1759 Charles Tait Graves and Alexander Macgillivray 2004 (n 699) 281.
1760 Charles Tait Graves and Alexander Macgillivray 2004 (n 699) 281.
1761 See chapter 4 § 4 E).

ing a process of trial and error), such a combination should not be eligible for protection. Linked with that, from a qualitative perspective, if the said combination does not confer any competitive advantage over the existing combinations used by other market participants, such a combination should not be deemed eligible for protection either, as the value it confers is minimal. Put simply, the combination of a specific "step of a process, part of a machine or design choice", for which a limited number of generally known or easily accessible alternatives exist with another set of known finite alternatives should be deemed to be generally known in the assessment of whether a combination trade secret exists.[1762]

The fourth principle propounds that courts should consider whether the defendant generated some of the elements of the combination independently. Graves considers this to be of utmost importance in the context of combination secrets mainly for three reasons: (i) if part of the information is already in the public domain, it is likely that the alleged misappropriator independently obtained the secret elements from public sources; (ii) if the information is common in trade with minor variations of the same basic elements, affirming protection may ultimately prevent competition among market participants; and (iii) if the defendant generated the information in an independent manner, the defendant may even file abusive litigation claims.[1763] Consequently, courts should always take into consideration whether the defendant has obtained the elements from which the combination is made from independent sources. This rationale was followed, for instance, by the District Court for the Northern District of Georgia in *Penalty Kick Management, Ltd. v. Coca-Cola Co*,[1764] where the defendant provided evidence that he had acquired the information from third party contractors. More complex appears the assessment of liability where some of the individual elements have been misappropriated, while others have been independently generated by the defendant. In this scenario, it is submitted that misappropriation should only arise with respect to the individual elements, provided that they meet the requirements for protection.[1765]

An additional principle is proposed here to avoid abusive litigation claims whereby, for the sake of legal certainty, the plaintiff must always be required to identify in a precise manner the information covered by the

1762 Charles Tait Graves and Alexander Macgillivray 2004 (n 699) 283.
1763 Charles Tait Graves and Alexander Macgillivray 2004 (n 699) 287.
1764 *Penalty Kick Management, Ltd. v. Coca-Cola Co,* 318 F. 3d 1284 (11th Cir. 2003); the facts of the case are summarised in chapter 4 § 4 C) II. 5. a).
1765 Charles Tait Graves and Alexander Macgillivray 2004 (n 699) 289.

trade secret, even though this is not explicitly mentioned in the TSD.[1766] Injunctions should not be granted unless the alleged infringer is informed of the information that he is free to use and that which is protected. Consequently, the individual elements that constitute the discrete entity that have been misappropriated should be clearly identifiable in the claims of the plaintiff.

As a final note, Graves holds that in order to find liability for trade secrets misappropriation, the plaintiff must prove that the defendant intended to acquire, use or disclose the combination as a whole.[1767] Under the legal framework created by the TSD, intent (or gross negligence) is only required in order to assess the liability of third parties. Consequently, such an interpretation is only supported in the present analysis with regard to acquisition by third parties.

6. Disclosures in the Cloud

a) General considerations and outline of the problem

Cloud computing has been defined as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (…) that can be rapidly provisioned and released with minimal effort or service provider interaction".[1768] In a more succinct fashion, the Commission has described it as "the storing, processing and use of data on remotely located computers accessed over the Internet", which "makes computing power available everywhere and to anyone".[1769] The widespread use of cloud computing services has brought about numerous advantages from an information management perspective. Two of the most salient ones are that the hardware is owned by the cloud computing service provider and that the computing capabilities can be accessed by the

1766 Unlike Article 1 (1)(i)(iii) TTBER.

1767 Charles Tait Graves and Alexander Macgillivray 2004 (n 699) 287.

1768 Peter Mell and Timothy Grance, 'The NIST Definition of Cloud Computing' (2011) The National Institute of Standards and Technology Special Publication 800-145, 2 <https://www.nist.gov/publications/nist-definition-cloud-computing> accessed 15 September 2018.

1769 Commission, 'Unleashing the Potential of Cloud Computing in Europe' COM(2012) 529 final.

user over the network at any time,[1770] which essentially has allowed companies and individuals to store large amounts of data in the cloud and at the same time reduce the expenses incurred in acquiring and maintaining costly computer systems.[1771]

The legal implications of cloud computing in the context of data protection and copyright law have been the object of in-depth analysis by both academia and legislators.[1772] However, its repercussions for the law of trade secrets have garnered substantially less academic attention, even though they are closely interconnected with the increasing security issues raised by cloud computing practices. In particular, two notable issues arise in connection with the eligibility of information stored in the cloud to be a trade secret, namely: (i) whether trade secrets lose their secret status upon being uploaded to computer servers owned by cloud service providers, and (ii) whether the contractual exemption of liability by cloud services providers in the case of misappropriation negates trade secrets protection on the basis that the trade secret holder had not adopted reasonable measures under the circumstances to protect them.[1773]

A survey of the standard terms and conditions that govern the service agreements between cloud service providers and their users reveals that while many service providers are willing to ensure the adoption of certain security measures, they frequently expressly disclaim liability for the confidentiality and security of the information stored in their services.[1774] In a similar vein, in a study published in 2012 on the negotiation of cloud con-

---

1770 Peter Mell and Timothy Grance, 'The NIST Definition of Cloud Computing' (2011) The National Institute of Standards and Technology Special Publication 800-145, 3 <https://www.nist.gov/publications/nist-definition-cloud-computing> accessed 15 September 2018.

1771 Sharon K. Sandeen 2014 (1522) 7-8.

1772 On the issues raised by data protection in the cloud see Kuan Hon and Christopher Millard, 'What is Regulated as Personal Data in Cloud Enviroments' 165-189 in Christopher Millard (ed), *Cloud Computing Law* (OUP 2013) and more generally the European Cloud Initiative <https://ec.europa.eu/digital-single-market/en/policies/cloud-computing> accessed 18 March 2018; on the issues raised by copyright in the cloud see Lothar Determann, 'What Happens in the Cloud: Software as a Service and Copyrights' [2015] 29 Berkeley Tech LJ 1095, 1121-1126.

1773 Georgios Psaroudakis, 'Trade Secrets in the Cloud' [2016] 38 EIPR 344, 346-347.

1774 Sharon K. Sandeen 2014 (1522) 32-38; Simon Bradshaw and others, 'Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services' (2010) Queen Mary School of Law Legal Studies Research Paper No. 63/2010, 21-22 <http://dx.doi.org/10.2139/ssrn.1662374>

tracts, the authors concluded that during the negotiation process, requesting full indemnification for breach of confidence could be a "show stopper" and, at most, cloud service providers agreed to a capped liability.[1775] The rationale underlying such a limitation is to restrict liability for any security breaches that may result in trade secrets misappropriation and compromise data integrity, in view of the sheer volume of information managed by data service providers.[1776]

Furthermore, keeping information confidential has become increasingly difficult in the cloud environment, as the relevant data flows from the holder to a third party (the cloud service provider).[1777] In the context of data protection laws, the European legislator has imposed higher obligations on the controller or processor, who need to adopt the necessary organisational and security measures to mitigate such risks, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing.[1778] In particular, the GDPR specifically refers to measures such as the encryption of personal data and the ability to ensure the confidentiality of processing services and systems.[1779] In line with this, it has been argued that if the information is encrypted before being uploaded to the cloud, there is no disclosure that affects the secret nature of the information and holders can still rely on trade secrets protection.[1780] However, while it is true that unauthorised access can be minimised or even avoided by using encryption methods before storing the in-

---

accessed 15 September 2018 noting that "The majority of providers surveyed expressly include terms in their T&C making it clear that ultimate responsibility for preserving the confidentiality and integrity of the customer's data lies with the customer. A number (for example, Amazon, GoGrid, Microsoft) assert that they will make "best efforts" to preserve such data, but nonetheless include such a disclaimer. A number of providers go so far as to recommend that the customer encrypt data stored in the provider's Cloud (for example, GoGrid, Microsoft) or specifically place responsibility on the customer to make separate backup arrangements".

1775 Kuan Hon, Christopher Millard and Ian Walden, 'Negotiating Cloud Contracts: Looking at clouds from both sides now' [2012] 16 Stanford Technology LR 79, 104-105.

1776 Sharon K. Sandeen 2014 (1522) 37.

1777 W Kuan Hon and Christopher Millard, 'Control, Security, and Risk in the Cloud' 18, 19-23 in Christopher Millard (ed), *Cloud Computing Law* (OUP 2013).

1778 According to Article 32 GDPR.

1779 Article 32(1)(a) and (b) GDPR.

1780 Georgios Psaroudakis, 'Trade Secrets in the Cloud' [2016] 38 EIPR 344, 346.

formation in the cloud, these practices do not completely exclude risks, because encryption methods can be "broken" or "cracked".[1781]

b) Guiding principles

Against this background, Sandeen argues that in the digital age careful attention should be paid to the way in which information flows and consequently she proposes a multifactor test in order to assess whether the storage of trade secrets in the cloud constitutes a disclosure that would prevent the application of the trade secrets liability regime, borrowing from privacy theories.[1782]

The first factor, the so-called "Public Policy Principle", distinguishes between disclosures that preclude the application of trade secrets rules from "mere transfers". Based on the definition provided by Black's Law Dictionary,[1783] the author suggests that while a disclosure consists of the transmission of knowledge, a "mere transfer" does not.[1784] Ultimately, she argues that such a distinction is in line with the principle that selling a product does not necessarily reveal all of the secrets therein enshrined.[1785] The second factor proposes to take into consideration the purpose of the transfer and more specifically the use of the cloud service by the uploading party. In particular, due account should be paid to whether the information stored in the cloud is shared within the company (inter enterprise) or with third parties that are under no duty of confidence.[1786] In the former case, it is less likely that the information will become generally known within the relevant circles, as employees are bound by a general duty of confidence. However, disclosure to third parties, such as contractors, clients or even cloud computing servers appears more problematic. The deciding factor should be whether the purpose of the transfer is to impart knowledge or to

1781 W Kuan Hon and Christopher Millard, 'Control, Security, and Risk in the Cloud' 18, 19 in Christopher Millard (ed), *Cloud Computing Law* (OUP 2013).
1782 Sharon K. Sandeen 2014 (1522) 81-84.
1783 According to Black's Law Dictionary, the term 'disclosure, v' refers to the "act or process of making known something that was previously unkown; a revelation of facts"; while the term "transfer, v" is defined as "to convey or remove from one place or one person to another; to pass or hand over from one to another" *Black's Law Dictionary* (9th edn, West Publishing 2009)
1784 Sharon K. Sandeen 2014 (1522) 88.
1785 Sharon K. Sandeen 2014 (1522) 88.
1786 Sharon K. Sandeen 2014 (1522) 89-90.

merely pass information from one server to another.[1787] The disclosure of secret information will negate trade secrets protection if the receiving party acquired actual knowledge of the information concerned under no duty of confidence. Hence, the trade secret holder will not be able to enforce secrecy or prevent further dissemination of the information, if he cannot prove that an implied duty of confidence existed.

The third factor suggests reviewing the representations of the cloud service provider to assess whether a relevant disclosure (and not a mere transfer) has occurred and, in particular, to evaluate whether employees or other third parties connected to the cloud server provider may have accessed the information.[1788] A similar rationale is followed under the fourth factor, which enquires into the "expectations of the uploading party". This is essentially understood to mean that trade secrets protection will only be available if the trade secret holder reasonably expected the cloud server provider to maintain secrecy regarding the information uploaded.[1789] This in turn is closely connected with the fifth requirement, which looks into the functionality of the cloud storage service and whether the processing of the information is automated or requires human intervention (for example, by employees of the cloud service provider). In the latter case, there may be a disclosure of information that may render unenforceable trade secrets liability rules. This is also linked to the sixth requirement proposed by Sandeen, which looks into the ability of cloud service providers to access and use stored data.[1790] The seventh and final principle propounds that due account should be paid to whether "the cloud storage service provider has not actually accessed, seen or used the stored information".[1791]

In the light of the above multifactor test, Sandeen proposes a four-step analytical framework to evaluate whether trade secrets protection is available to information stored in the cloud. Accordingly, the first step consists of assessing whether information is transmitted beyond servers owned by the trade secret holder.[1792] The second step enquires into the nature of the flow of information and whether there was an actual disclosure or just a "mere transfer", pursuant to the proposed multifactor-test outlined

1787 Sharon K. Sandeen 2014 (1522) 89-90.
1788 Sharon K. Sandeen 2014 (1522) 89-90.
1789 Sharon K. Sandeen 2014 (1522) 92-93.
1790 Sharon K. Sandeen 2014 (1522) 96.
1791 Sharon K. Sandeen 2014 (1522) 97-98.
1792 Sharon K. Sandeen 2014 (1522) 99-100.

above.[1793] The third step analyses whether a duty of confidentiality (implied or express) exists between the cloud service provider and the trade secret holder.[1794] Finally, the fourth factor examines the measures adopted by the trade secret holder in order to preserve its trade secrets.[1795]

As a whole, it is submitted that the distinction proposed by Sandeen regarding "mere transfers" and "disclosure" seems to provide a convincing starting point to assess whether the information stored in the cloud is eligible for trade secrets protection. Only an actual transfer of knowledge between a trade secret holder and a cloud service provider or any other third party may constitute a relevant disclosure that prevents the application of trade secrets liability rules, unlike passive transmissions. Similarly, it appears of utmost importance to look into the purpose of the transfer and the functionalities of the cloud service in order to examine the nature of the disclosure, how the information is stored and who has access to it. Indeed, most cloud service providers do not have an interest in, and do not gain knowledge of, the information stored in their servers. They merely store it in a passive manner. Consequently, it is submitted here that even in the absence of express confidentiality obligations agreed upon contractually, if a cloud service provider merely stores the information passively without accessing it, the information maintains its secret nature and any unauthorised acquisition by a third party will trigger liability. This is furthermore indicated in Recital 39 GDPR, which provides that personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data.

In this context, it is argued that the analytical framework suggested by Sandeen places too much relevance on the adoption of reasonable measures under the circumstances requirement and the representations of the cloud service providers. As outlined above, in most EU jurisdictions, such a requirement is either non-existent (England) or the threshold is extremely low (Germany).[1796] As has been suggested, interpreting such a requirement in a very demanding manner would lead to an overinvestment in protective measures and spur an arms race among competitors.[1797] Hence, the fact that a cloud service provider undertakes to adopt security measures to preserve confidentiality (which is furthermore mandated by the GDPR

1793 Sharon K. Sandeen 2014 (1522) 100-101.
1794 Sharon K. Sandeen 2014 (1522) 101.
1795 Sharon K. Sandeen 2014 (1522) 102.
1796 See chapter 4 § 3 E).
1797 See chapter 4 § 3 E).

with respect to personal data) but disclaims liability for any breach should not automatically preclude trade secrets protection based on the fact that the trade secrets holder failed to adopt reasonable measures under the circumstances.[1798] However, in the unlikely event that no security measures are adopted by the cloud service provider, it is submitted here that the encryption of the information before its storage in the cloud by the trade secret holder should suffice to maintain the undisclosed nature of the information. In both scenarios, unauthorised access to the stored data (as well as any subsequent use or disclosure) by a third party that uses unlawful means to acquire the information, such as hacking the account of the user, will trigger liability under the trade secrets legal regime.

In any event, in the interest of legal certainty, it seems highly advisable that users obtain an express agreement from the cloud service provider, by virtue of which the latter undertakes to treat the information stored in its server in a confidential manner and not to disclose it to any third parties beyond its employees and on a "need-to-know" basis, even if liability in the event misappropriation is excluded. In such a contract, the trade secret holder should demand that the cloud server provider adopt reasonable security measures, in line with the requirements established in the GDPR for personal data.

In sum, the disclosure of information to the cloud service provider should not be regarded as automatically secrecy-destroying. The better view is that only the disclosure of information that involves the transfer of knowledge between parties that are not bound by a confidentiality obligation should be relevant. Furthermore, disclaimers of liability in the case of unauthorised access shall not prevent the application of trade secrets protection against third parties that access the information unlawfully.

D) The doctrine of relevant circles

The corollary of the relative secrecy approach is that a certain number of people can access and acquire actual knowledge of the information covered by a trade secret. Yet again, the difficulty lies in establishing when the number of recipients is such that the information becomes generally known. Resorting to a numerical value in abstract (quantitative approach)

1798 Amazon Web Service User Agreement, para 3.1 <https://d1.awsstatic.com/legal/awsamendedCAterms/AWS%20Amended%20CA%20Terms_es.pdf> accessed 15 September 2018.

does not seem the most adequate solution, as the assessment of secrecy is largely factually driven. Article 39(2) TRIPs and Article 2(1)(a) TSD do not provide further guidance in this regard, as they only mention that information should not be known among, or be readily accessible to, "*persons within the circles that normally deal with the kind of information in question*". This statement seems to indicate that protection ceases if information is not known by the general public, but is known among members of a specific industry.[1799] Such a requirement seems to evocate the "person having ordinary skills in the art" standard applied in patent law. For secrecy to be lost the recipient of the information must "have access to normal sources of specialised information",[1800] which in turn seems to imply that he must be able to understand the content of the disclosure (in the transfer of knowledge sense). Indeed, not every member of the general public can comprehend the content of technical disclosures. By way of illustration, the publication of a complex biotechnological invention will only be understood by those with the necessary technical knowledge.

In view of the interpretative difficulties raised by the so-called "doctrine of relevant circles", the following sections explore how courts and commentators in three different jurisdictions (U.S., England and Germany) have interpreted such a condition in order to extract the applicable guiding principles (section IV).

I. U.S.

In the U.S, the commentary to the UTSA notes that secrecy is lost when the information is generally known or readily accessible by "principal persons(s) who can obtain economic benefit from information".[1801] The

1799 François Dessemontet 2008 (n 601) 283.

1800 Daniel Gervais 2012 (n 505) para 2.486; conversely, Thomas Reimann 1998 (1323) 298, 299.

1801 See UTSA Comment to § 1 according to which: "The language 'not being generally known to and not being readily ascertainable by proper means by other persons' does not require that information be generally known to the public for trade secret rights to be lost. If the principal person / persons who can obtain economic benefit from information is / are aware of it, there is no trade secret"; see further the Restatement (Third) of Unfair Competition §39 (Am. Law Inst. 1995) comment f noting that "limited non-confidential disclosure will not necessarily terminate protection if the recipients of the disclosure maintain the secrecy of the information".

Supreme Court has further noted that relative secrecy should be assessed against the knowledge of "industry members".[1802] A review of the relevant case law suggests that courts have taken mostly two approaches when assessing from a qualitative and quantitative perspective the extent of the disclosure that renders a trade secret unprotectable. According to the first interpretation, when the majority of persons within an industry are aware of the information, protection ceases.[1803] Pursuant to the second interpretation, protection lasts until all of the members of an industry are aware of the information and consequently any competitive advantage derived from the information being kept secret disappears.[1804] In this context, due to the progressive erosion of secrecy, Unikel refers to trade secrets as "disappearing rights"[1805] and proposes an analytical framework that distinguishes between three categories of information:

– The first one, "Category 1" encompasses information that is known to substantially all persons in a particular field or industry;
– The second type, "Category 2" refers to information that is known to a majority but unknown to a minority;
– The third type, "Category 3" refers to information that is known to a minority but unknown to a majority.[1806]

Evidently, information in Category 1 falls outside the scope of trade secrets protection because it provides no competitive advantage to its holder.[1807] Conversely, information in Category 3 confers a notable competitive edge and, accordingly, is regarded as eligible for protection. The assessment of the level of protection that corresponds to Category 2 seems more problematic because its absolute competitive value is lower than in Category 3, but it may still possess relative value.[1808] In this context, Unikel suggests that only Category 3 information should be protected and that the term "minority" should be construed as meaning "less than half of persons who

1802 The Supreme Court has clearly enshrined this principle in two of its main decisions on trade secrecy law. In *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986, 1002 (1984) it noted that "Information that is public knowledge or that is generally known in an industry cannot be a trade secret".
1803 See in this regard *TGC Corp. v. HTM Sports, B.V.*, 896 F. Supp. 751, 759-760 (E.D. Tenn. 1995).
1804 *Wilson. v. Barton & Ludwig Inc*., 296 S.E.2d 74, 75 (Ga. Ct. App. 1982).
1805 Robert Unikel 1998 (n 1512) footnote 142.
1806 Robert Unikel 1998 (n 1512) 844.
1807 Robert Unikel 1998 (n 1512) 850.
1808 Robert Unikel 1998 (n 1512) 854.

could obtain economic or competitive value from its use".[1809] Even though such a proposition appears to provide great legal certainty for the trade secret holder and the alleged misappropriators, in certain industries the competitive advantage conferred by a trade secret known among, for instance, 40% of the market participants may be rather low, particularly if alternative inventions exist. Additionally, 55% of the market participants in a given industry may have obtained a secret in confidence as a result of a licensing agreement. Under Unikel's approach, one could argue that the licensing agreement should be regarded as null and void because the object of the contract has ceased to exist, even though the trade secret holder retains control over the undisclosed nature of the information.

II. England

On the other side of the Atlantic, several English decisions have suggested that a piece of information enters the public domain when the information can be accessed "by those who have an interest in knowing it".[1810] This was for instance the deciding factor in *Franchi v Franchi*,[1811] where the High Court of Justice of England and Wales regarded a patent specification published in Belgium as generally known because patent attorneys regularly checked foreign specifications. In a similar vein, the Law Commission noted that "much information which is technically available to the public is not generally known and may in fact be known only to a handful of people".[1812] In this context, several cases allude to the fact that the accessibility of information will ultimately depend upon the skill and knowledge of the person that obtains it.[1813] For instance, Jacob J in *Cray Valley Ltd v Deltech Europe Ltd*, a case concerning the misuse of confidential information regarding formulations of resins and their manufacturing instructions, noted that "the recipes in issue here, although not published to the world in full, are to those skilled in the art of resin manufacture and

1809 Robert Unikel 1998 (n 1512) 875.
1810 Lionel Bently and Brad Sherman 2014 (n 125) 1149.
1811 *Franchi v Franchi* [1967] RPC 149 (Ch).
1812 Law Commission, *Working Paper on Breach of Confidence* (Law Com No 58 1974) 102 (as cited in Roger M. Toulson and Charles M. Phipps 2012 (n 326) para 3-116).
1813 A Roger M. Toulson and Charles M. Phipps 2012 (n 326) 3-116 with further references.

design, very ordinary".[1814] This statement seems to indicate that in England, at least in the case of technical information, the relevant factor in assessing secrecy is whether the information is accessible to people in a specific field. Such a statement highlights that the deciding factor that renders information unprotectable is the acquisition of actual knowledge beyond mere factual access to the information.

III. Germany

Pursuant to the definition followed by German case law, for information to be considered secret it must be "known only to a narrow limited number of persons".[1815] Against this background, German commentators have identified four potential normative standards that allow for delineating when information enters the public domain in a more precise manner. Such principles will guide the present discussion.[1816]

In the first place, to maintain secrecy, information should only be shared with a limited circle of confiders ("*Begrenztheit des Mitwisserkreises*"). Accordingly, trade secrets should only be imparted to a restricted number of persons.[1817] However, such a standard is seemingly vague and open-ended because no hint as to the precise number of persons or the relationship among them can be inferred from it.[1818] Thus, in an attempt to provide more precision, some commentators have argued that the most appropriate yardstick should be that the trade secret holder has *control* over the relevant circles that know and have access to the information concerned ("*Kontrollierbarkeit des Mitwisserkreise*").[1819] Such an approach provides greater legal certainty, as it simplifies the proof hurdle. Indeed, confidentiality obligations that stem from labour contract or specific contractual NDAs are generally regarded as having sufficient probative value.[1820] Notwithstanding this, in the event of independent discovery by another competitor, the holder who first developed the secret may lose control de-

1814 *Cray Valley Ltd v Deltech Europe Ltd* [2003] EWHC 728 (Ch) [55].
1815 Translation by Gintare Surblyte 2011 (n 182) 49; BGH MMR 2006, 815, 816 – *Kundendatenprogramm*.
1816 Björn H. Kalbfus 2011 (n 1300) 85.
1817 BGH GRUR 1964, 31, 32 – *Petromax II*; BGH GRUG 1955, 424, 425 – *Möbelpaste*; *Köhler*/Bornkamm/Feddersen (n 835) § 17 Rdn 7a.
1818 Björn H. Kalbfus 2011 (n 1300) 86.
1819 See Rudolf Kraßer 1977 (n 1327) 179; *Ohly*/Sosnitza (n 813) § 17 Rdn 8.
1820 *Ohly*/Sosnitza (n 813) § 17 Rdn 8.

pending on the use that the latter makes of the information and the subsequent acquisition of the secret by lawful means.[1821]

The third interpretation regards that the doctrine of relevant circles in fact refers to the ignorance of the trade secret holder's competitors ("*Unkenntnis seitens der Wettbewerber*").[1822] On the one hand, it is clear that when all of the competitors in a market are aware of the information covered by a specific trade secret such information can no longer qualify as undisclosed.[1823] On the other, it is also true that if two competitors in a big market have developed the same trade secret independently, it retains the necessary quality of confidence. In such a scenario, with time, when more competitors are able to create it independently, the secret will erode and will end up entering the public domain. Furthermore, the economic value (understood in terms of a competitive advantage) will also decrease over time.[1824] Yet, it seems too strict (or unrealistic) to consider that secrecy is not lost until the last competitor is aware of it.[1825] For instance, in a market made up of fifty participants, if more than half of them are aware of the information it seems unlikely that courts will still regard it as secret. Another hurdle posed by this standard is that it overlooks the fact that often competitors cooperate in the context of research and development projects or strategic alliances, in which they share secret commercial and technical information. If information could not retain its secret nature, cooperation among enterprises would be hindered, thus negatively affecting innovation.[1826]

1821 As identified by Björn H. Kalbfus 2011 (n 1300) 86.

1822 Thomas Reimann 1998 (1323) 300 where the author notes that in Germany the protection of trade secrets is regulated by the UWG, which ultimately protects fair competition among market participants.

1823 François Dessemontet 2008 (n 601) 284.

1824 Rudolf Kraßer 1970 (n 831) 588; Gintare Surblyte, 'Enhancing TRIPS: Trade Secrets and Reverse Engineering' 725, 737 in Hanns Ullrich and others (eds), *TRIPS plus 20 – From Trade Rules to Market Principles* (Springer 2016).

1825 On the contrary, Nuno Pires de Carvalho 2008 (n 529) para 39.2.54 notes that "Secrecy, under subparagraph (a), remains until the last competitor (or the last person within the circle that normally deals with that information) obtains the desired information. If there are ten firms competing in a certain market, and nine of them know (secretly) about a process whereas the tenth does not know it, nor has it access to the information, that information is a trade secret as far as the tenth company is concerned. The important aspect is that information be not readily available to that tenth company (for example, as a result of its having been published in a scientific magazine, of which the company is not aware".

1826 Björn H. Kalbfus 2011 (n 1300) 88.

Finally, the fourth propounded principle is that information remains secret as long as the holder and the recipients of the information have a common interest in keeping it undisclosed.[1827] Such an assessment is not factually driven, and furthermore it introduces a subjective element in the interpretation of secrecy. In addition, it does not apply in cases of utmost practical relevance, such as in the relationship between an employer and an employee, particularly after the termination of the employment relationship.[1828]

IV. Guiding principles

In sum, it seems that ultimately the most appropriate principle is the one that focuses on the assessment of the control of information disclosed by the trade secret holder, together with the possibility that the circles that actually have access to the said information are able to acquire active knowledge of it because it relates to their field of expertise.

Indeed, information will retain its secret nature provided that the trade secret holder retains control over the use and subsequent disclosure of the information concerned within the relevant circles, for instance through contractual NDAs. This ensures that the company will maintain its competitive advantage derived from the secrecy of the information for as long as it takes competitors to reverse engineer the product. It is also in line with Article 2(2) TSD, which defines the trade secret holder as the "natural or legal person *lawfully* controlling a trade secret".

With respect to the acquisition of knowledge, it should be noted that the disclosure of complex technical secrets, such as a chemical formula, should not be regarded as secrecy-destroying, unless the recipients of the information are capable of understanding the content of the secret and acquire active knowledge of it. Consequently, if the said formula is disclosed to lawyers with no chemical background in the course of a compliance process, it should not be regarded as publicly known for the purposes of assessing secrecy, unless it is further disseminated to parties that can comprehend it. In a similar vein, the assessment of secrecy should always be considered against the knowledge in the relevant industry in order to prevent the privatisation of information already in the public domain. Ultimately, such a rationale corresponds to the principle outlined with regard

1827 Björn H. Kalbfus 2011 (n 1300) 87.
1828 Björn H. Kalbfus 2011 (n 1300) 87.

to cloud disclosures, by virtue of which the disclosure of encrypted information does not render the information generally known.[1829]

E) Secrecy as opposed to IPRs normative standards

Chapter 1 highlighted that one of the essential differences between trade secrets and formal IPRs is that to merit protection information must meet a certain qualitative threshold. In the case of patents, the information they protect must be novel and inventive. Similarly, works protected under copyright rules must be original. By contrast, in the case of trade secrets, information is protected merely by being kept undisclosed. The general principle is that no qualitative restriction beyond secrecy is required. Notwithstanding this, in a number of decisions courts in England and the U.S. have used a language that points to the introduction of limitations regarding the type of information protected, which is sometimes required to be "novel" or "original". The following sections examine the actual meaning and effects of such limitations with regard to the novelty requirement in patent law (section I) and originality in copyright law (section II). Finally, section III concludes.

I. Novelty

The concept of disclosure is central for the appraisal of secrecy in the context of trade secrets and novelty in the realm of patent law.[1830] The following sections underscore the differences and similarities between the two requirements in the light of the normative framework created by the EPC (section 1) and proceed to study the most relevant cases that demand novelty in the U.S. (section 2) and in England (section 3).

1. Novelty under the EPC

As stated above,[1831] Article 54 EPC sets forth that for an invention to be novel it must not form part of the state of the art. The EPC is governed by

1829 Chapter 4 § 4 C) II. 6. b).
1830 Thomas Reimann 1998 (1323) 298.
1831 See chapter 1 § 3 A) I. 1.

the principle of "objective novelty", which is also referred to as "absolute novelty".[1832] Accordingly, patent applications are to be examined against all of the information available on the priority date, which may have been published all over the world.[1833] Furthermore, and to avoid double patenting, Article 54(3) EPC creates a legal fiction whereby patent applications filed before the relevant priority date, but published on or after that date, form part of the state of the art. Thus, under the legal framework set forth in Article 54 EPC, obscure sources are considered novelty-destroying.[1834] Furthermore, the EPO follows a strict novelty approach, by virtue of which a document is only considered novelty-destroying if all of the elements of a claim are disclosed in the document "combined within the same context".[1835]

Drawing on the foregoing analysis, the secrecy requirement has often been equated with novelty in patent law, mostly owing to the fact that trade secrets require that their object of protection is not generally known.[1836] Just as patents should not be granted over inventions already in the public domain, trade secrets should not be afforded protection if their subject matter is public.[1837] To hold otherwise would amount to a privatisation of public information.

Notwithstanding this, there seems to be a consensus regarding the fact that unlike the novelty standard in patent law, the secrecy requisite is not an absolute one.[1838] As a result, the assessment of these two requirements of protection should be different under the two different legal regimes in place. With regard to patents, as already discussed, a number of decisions from the Enlarged Board of Appeals of the EPO have established that it is not required that a person may in fact examine the prior art document or have reason to do so.[1839] By contrast, in the case of trade secrets the publication of "prior art information" is not necessarily immediately secrecy-de-

1832 Also in UK Patents Act 1977 (s 2) and German Patent Act (§ 1(1)).
1833 No geographical limits apply.
1834 Lionel Bently and Brad Sherman 2014 (n 125) 534.
1835 Alexander Harguth and Steven Carlsson, *Patents in Germany and Europe* (2nd edn, Wolters Kluwer 2017) 74; EPO T 0931/92 (10 August 1993).
1836 François Dessemontet 2008 (n 601) 282; Gerald Reger 1999 (n 553) 261 holds a different view and argues that the "not generally known or readily accessible" requirement is to be construed as a factual requirement with no normative value.
1837 François Dessemontet 2008 (n 601) 282.
1838 *Harte-Bavendamm*/Henning-Bodewig (n 376) § 17 Rdn 4.
1839 Chapter 1 § 3 I; Lionel Bently and Brad Sherman 2014 (n 125) 532; G 1/92 [1993] OJ EPO 277, 279 noting that "it is the fact that direct and unambiguous

stroying.[1840] Such an appraisal should be carried out on a case-by-case basis, as it does not suffice that the information is merely theoretically accessible. It is a matter of degree; it depends on the likelihood that a third party will access the theoretically generally available sources.[1841] Against this background, it has been submitted that the "not readily accessible or generally known" requirement refers to the specific possibility of third parties acquiring the information such that it is regarded as known or "knowable".[1842] Such a test is of a factual nature and unlike the novelty requirement in patent law has no normative value.[1843] Ultimately, the assessment of secrecy will depend on the possibility that the trade secret holder can exercise control over the use and subsequent disclosure of the information for which protection is sought.

The absolute nature of the novelty standard under patent law has not been without criticism, particularly in the light of the vast amount of data available through the Internet and the fact that the relevant yardstick is not actual disclosure but potential accessibility by any member of the public. In view of this, the EPO Technical Board of Appeal, in a decision concerning Internet disclosures, held that for the purpose of assessing novelty, a specific document should be accessible in a direct and unambiguous manner by known means and methods.[1844] In such a context, the proposed test is that the document (i) can be found by looking up the main keywords related to the content on a search engine, and (ii) is accessible at a URL for a period of time long enough for a person under no confidentiality obligation to access it.[1845] These requirements present some clear parallels with the sequential preservation model discussed above with regard to Internet disclosure and its effects on secrecy.[1846] Yet, while in the context of patent

---

access to some particular information is possible, which makes the latter available, whether or not there is any reason for looking for it".

1840 Rudolf Kraßer 1970 (n 831) 590.

1841 François Dessemontet 2008 (n 601) 282; similarly, Ansgar Ohly 2014 (n 100) 4: "Im Gegensatz zum Neuheitsbegriff des Patentrechts entfällt der Geheimnischarakter nicht schon automatisch dann, wenn die Information aus allgemeinzugänglichen Quellen verfügbar ist, denn es geht nicht um abstrakte Zugänglichkeit, sondern um leichte Zugänglichkeit im konkreten Fall".

1842 Elizabeth A. Rowe and Sharon K. Sandeen, *Trade Secrecy and International Transactions* (Edward Elgar 2015) para 3.18.

1843 Gerald Reger 1999 (n 553) 261.

1844 EPO T 1553/06 (12 March 2012).

1845 EPO T 1553/06 (12 March 2012); see further Guidelines for Examination in the EPO, Part G, Chapter IV. Section 7.5.

1846 See chapter 4 § 4 C) II. 4. d).

law the relevant issue is merely that the information is available for a period sufficiently long to allow for potential access by any member of the public, in the context of trade secrets due account should be paid to the extent of the actual disclosure and, in particular, the specific traffic of the website. In addition, the recipient's reason to know that the information was a trade secret also plays a role in the assessment of secrecy vis-à-vis the infringer, whereas such subjective considerations are not relevant in the assessment of the novelty standard.

In the light of the above, the following sections analyse the facts and legal reasoning followed by the most relevant decisions in the U.S. and England that have required that information should be novel, in order to shed light on the actual contours of secrecy and its intersection with the novelty requirement.

2. U.S. cases that demand novelty

a) Analysis of the relevant case law

The U.S. Supreme Court, in its landmark decision regarding the potential pre-emption of trade secrets state law by federal patent law, *Kewanee Oil Co. v. Bicron Corp*, held that "novelty in the patent law sense, is not required for a trade secret.(…) However some novelty will be required if merely because that which does not possess novelty is usually known; secrecy, in the context of trade secrets, thus implies at least minimal novelty".[1847]

The aforementioned statement has been greatly influential and cited by a number of subsequent decisions, such as the 1980 decision of the District Court in Pennsylvania, *Anaconda Company v. Metric Tool & Die Company*.[1848] This case concerned the alleged misappropriation of the secret design of a machine used to manufacture telephone cord armour that protected public telephones from wear and tear by a former employee of the plaintiff.[1849] In the assessment of whether the machine in fact constituted a

1847 *Kewanee Oil Co. v. Bicron Corp., Kewanee Oil Co. v. Bicron Corp.,* 416 U.S. 470, 474 (1974).

1848 *Anaconda Company v. Metric Tool & Die Company*, 485 F. Supp. 410 (E.D. Pa. 1980).

1849 *Anaconda Company v. Metric Tool & Die Company*, 485 F. Supp. 410, 413 (E.D. Pa. 1980).

trade secret the court noted that "novelty is only required of a trade secret to the extent necessary to show that the alleged secret is not a matter of public knowledge.(…) A trade secret may be no more than a slight mechanical advance over common knowledge and practice in the art".[1850] Consequently, the court affirmed the existence of a trade secret because the precise configuration and assembly of the components made the machine "unique".[1851]

Following an analogous rationale, the United States Courts of Appeals of the Sixth Circuit ruled in *Richter v. Webstab, Inc*[1852] that an idea to include notebook covers and binders that matched trendy clothing was not protectable because it did not present sufficient "novelty".[1853] More specifically, it was argued that the idea of "using a particular design on a particular item is abstract" and consequently if the "design is not novel no legal protection is available".[1854] In addition, the court went on to note that:

> The law does not favour the protection of *abstract ideas as the property of the originator*. An idea should be *free for all to use* at least until someone is able to translate such an idea into a sufficiently useful form that it may be patented or copyrighted. Thus, competition in the use of ideas is a social good, hastening the process of innovation (emphasis added).[1855]

Thus, it was concluded that denying legal protection to abstract ideas disclosed in confidence would not have a negative impact on the flow of ideas among companies, because businesses had an interest in commercially exploiting a product, not the underlying concept.[1856]

Similar considerations were applied in a decision affecting the audiovisual industry with regard to the protection of an idea for a television series. In *Murray v. National Broadcasting Company*[1857] the Court of Appeals

---

1850 *Anaconda Company v. Metric Tool & Die Company*, 485 F. Supp. 410, 422 (E.D. Pa. 1980).

1851 *Anaconda Company v. Metric Tool & Die Company*, 485 F. Supp. 410, 422 (E.D. Pa. 1980); similar considerations apply in *Nickelson v. General Motors Corporation*, 361 F.2d 196, 199 (7th Cir. 1966), where the court noted that "trivial advances or differences in formulas or process operations are not protectable as a trade secret".

1852 *Richter v. Westab, Inc.,* 529 F.2d 896 (6th Cir. 1976).

1853 *Richter v. Westab, Inc.,* 529 F.2d 896, 901 (6th Cir.1976).

1854 *Richter v. Westab, Inc.,* 529 F.2d 896, 901 (6th Cir. 1976).

1855 *Richter v. Webstab, Inc.,* 529 F.2.d 896, 901 (6th Cir.1976).

1856 *Richter v. Westab, Inc.,* 529 F.2d 896, 901 (6th Cir. 1976).

1857 *Murray v. National Broadcasting Co., Inc.,* 844 F.2.d 988 (2d Cir. 1988).

of the Second Circuit ruled that an idea to create a sitcom that portrayed a black family in non-stereotypical roles (The Bill Cosby Show) could not be protected as a trade secret because it lacked "novelty".[1858] In this regard, the court argued that television networks had already cast black actors and that the idea for such a show had been suggested by Bill Cosby himself before the plaintiff, a former employee of the defendant (a television network), had submitted it for consideration to the executives of the network.[1859] In addition, it was noted that the plaintiff "had confused an idea with its execution"[1860] and that "when an idea consists in essence of nothing more than a variation on a basic theme (…) novelty cannot be found to exist".[1861] Against this background, it was concluded that to be protected, ideas must reflect a "genuine novelty and invention".[1862] Otherwise, they should be regarded as being in the public domain and free for everyone to use.

In view of the above, it appears that courts in the U.S. have demanded a certain threshold of novelty in trade secrets litigation mostly in two scenarios. First, it has been required in cases concerning manufacturing industries where the alleged trade secret was just a minor and often self-evident variation of existing technical solutions. Secondly, courts also seem to rely on novelty to prevent the monopolisation of abstract ideas by alleged trade secret holders.[1863] This is closely connected with the so-called "law of ideas", which is examined in the following section.

b) The "law of ideas"

The analysis of the novelty requirement under U.S. trade secrets law would not be complete without referring to the emergence of a field of law dur-

1858 *Murray v. National Broadcasting Co., Inc.*, 844 F.2.d 988, 991 (2d Cir. 1988).
1859 *Murray v. National Broadcasting Co., Inc.*, 844 F.2.d 988, 991 (2d Cir. 1988).
1860 *Murray v. National Broadcasting Co., Inc.*, 844 F.2.d 988, 992 (2d Cir. 1988).
1861 *Murray v. National Broadcasting Co., Inc.*, 844 F.2.d 988, 993 (2d Cir. 1988).
1862 *Murray v. National Broadcasting Co., Inc.*, 844 F.2.d 988, 993 (2d Cir. 1988).
1863 James Pooley 2002 (n 66) § 4.03[1]; along the same lines the Restatement (Third) of Unfair Competition § 39 comment f concludes that "although trade secrets cases sometimes announce a "novelty" requirement, the requirement is synonymous with the concepts of secrecy and value described in this Section and the correlative exclusion of self-evident variants of the known art".

ing the second half of the XX century known as the "law of ideas".[1864] In essence, such a body of case law was developed under common law principles to address situations where the originator of an idea conveyed it to a third party, who eventually went on to exploit it without authorisation from the originator and without providing adequate compensation.[1865] In such cases, courts resorted mostly to five legal theories (the contours of which are sketchy) to provide legal redress to the originator and allow him to recover the value of his idea. The five causes of action most frequently invoked were: (i) express and (ii) implied contracts, whereby the defendant explicitly or implicitly undertook to pay a certain amount as consideration for the disclosure of the idea; (iii) property theories over the idea that prevented its unauthorised use; (iv) quasi-contract and unjust enrichment doctrines based on fairness arguments, and (v) breach of confidence, which to a large extent overlapped with trade secrets protection. These five doctrines have been the object of vehement criticism by legal commentators, mostly due to the potential disruptive effects that the "law of ideas" may have regarding the balance struck by intellectual property law and the public domain and the negative impact on innovation and creativity.[1866] Indeed, the increasing relevance of the "law of ideas" during the second half of the XX century is most adequately explained by the prevalence of the Restatement (First) of Torts, which required that a trade secret was "used in one's business".[1867] To be more precise, the comments to the Restatement noted that "a trade secret is a process or device for continuous use in the operation of the business".[1868] Consequently, courts regarded that ideas submitted for consideration to prospective business partners did not qualify for trade secrets protection, because the disclosure of the idea would not provide a continuous competitive advantage and the commercial exploitation of the products in which they were embodied rendered them generally known.[1869]

Notwithstanding the aforementioned, for the purposes of the present analysis, it is worth noting that a common threat to the five underlying

1864 James Pooley 2002 (n 66) § 4.03[1]; Margreth Barrett, 'The "Law of Ideas" Reconsidered' [1989] 71 J Patent & Trademark Office Society 691, 692.
1865 Margareth Barret 1989 (n 1864) 692.
1866 Melville B. Nimmer, 'The Law of Ideas' [1954] 27 Southern California LR 119, 120-140; Margareth Barret 1989 (n 1864) 757; Robert Denicola, 'The New Law of Ideas' [2014] 28 Harvard Journal of Law & Technology 195, 220-225.
1867 Restatement (First) of Torts § 757 (Am. Law Inst. 1939) comment b.
1868 Restatement (First) of Torts § 757 (Am. Law Inst. 1939) comment b.
1869 Robert Denicola 2014 (n 1866) 198-199.

theories of the "law of ideas" was that to merit protection courts required information to be *novel* and *concrete*.[1870] The *novelty* requirement was mostly interpreted with a two-fold meaning. Ideas should: (i) be either original to the plaintiff or (ii) be innovative in character (i.e. not part of the public domain), or (iii) fulfil a combination of both requirements.[1871] The first interpretation of the novelty requirement was fiercely criticised, because it allowed for privatising information that was in fact in the public domain but unknown to a minority, the alleged originator.[1872] As regards *concreteness*, case law did not provide a uniform interpretation of its conceptual contours.[1873] A number of judges understood that the idea should be presented in a tangible form or in writing, whereas some stressed that only the tangible form in which the idea was expressed would merit protection.[1874] Others held that *concreteness* should be understood as meaning that the idea should be fully developed.[1875] The latter view seems better suited to finding an equilibrium between the public domain and the interests of idea originators in recovering the cost of development of such ideas. In fact, similar considerations have been followed by English courts under the breach of confidence action.[1876]

As a final note, the enactment of the UTSA in the 1980s and more recently the DTSA, which do not require "continuous use of the secret", have allowed for overcoming the definitional problems raised by the Restatement (First) of Torts. Consequently, courts have progressively abandoned the five legal theories that dominated the "law of ideas" and subsumed such controversies under the law of trade secrets.[1877] In turn, the *novelty* and *concreteness* requirements have gradually been replaced by the

---

1870 Melville B. Nimmer 1954 (n 1866) 140.
1871 Margareth Barret 1989 (n 1864) 711.
1872 Margareth Barret 1989 (n 1864) 711.
1873 For a review of the first decisions on this topic see Melville B. Nimmer 1954 (n 1866) 140-144; Lionel S. Sobel, 'The Law of Ideas, Revisited' [1994] 1 UCLA Entertainment LR 9, 21-32.
1874 Margareth Barret 1989 (n 1864) 712-713 with further references.
1875 For instance, in *Smith v. Recrion Corporation,* 541 P.2d 663, 665 (Nev. 1975) the Supeme Court of Nevada noted that: "Concreteness pertains to the developmental stage of the idea, i.e., the idea must be sufficiently developed as to constitute a protectable interest. An ida in order to meet the test of concreteness must be ready for immediate use without any additional embellishment. The purpose of the test is to insure that the idea merits protection: That is tangibe and would not exist but for the independent efforts of its author".
1876 As examined in chapter 4 § 4 E) II. 2.
1877 Robert Denicola 2014 (n 1866) 236.

three traditional requirements under the law of trade secrets, whereby in order to merit protection, an idea must be secret, present commercial value due to its undisclosed nature, and be subject to reasonable steps under the circumstances to maintain its secret nature.[1878]

3. English cases that demand novelty under the breach of confidence action

In England, "novelty" has frequently been used to assess the protectability of secrets comprised of elements solely in the public domain (combination secrets), but also in manufacturing industries.[1879] As regards the first category, in the famous English case *Coco v Clark*,[1880] Megarry J indicated that the quality of confidence stemmed from a process of the human brain that conferred novelty, originality or even ingenuity:

> Something that has been construed solely of the materials in the public domain may possess the necessary quality of confidentiality: for something *new and confidential* may have been brought into being by the *application of the skill and ingenuity of the human brain*. *Novelty* depends on the thing itself, and not upon the quality of its constituent parts. Indeed, often, the more striking the novelty, the more commonplace its components… *whether it is described as originality or novelty or ingenuity or otherwise, I think there must be some product of the human brain which suffices to confer a confidential nature upon the information* (emphasis added).[1881]

In the same vein, in *Coulthard v Disco Mix Club Ltd*.[1882] the plaintiff, a DJ, brought legal action for breach of confidence against his former DJ partners. He claimed, among other arguments, that the defendants were using a technique that he had developed for creating a beat-mix sound file that he had disclosed in confidence in the course of a partnership agreement. While delivering its judgement, the Court held that the techniques were "pretty obvious" and therefore not protectable.[1883]

1878 Robert Denicola 2014 (n 1866) 236.
1879 Lionel Bently and Brad Sherman 2014 (n 125) 1156.
1880 This case is analysed in chapter 3 § 3 C) II.
1881 *Coco v A.N.Clark (Engineers) Ltd* [1969] RPC 41, 47.
1882 *Coulthard v Disco Mix Club Ltd* [2000] 1 WLR 707 (Ch).
1883 *Coulthard v Disco Mix Club Ltd* [2000] 1 WLR 707 (Ch), 726.

II. Originality

In England, as well as in the U.S., some courts have ruled that for information to be protected under the breach of confidence action it should be deemed "original".[1884]

As is examined in chapter 5[1885] in the context of perfumes, originality is also one of the criteria for protection under copyright law. So far, the originality benchmark has not been harmonised as such, either across the EU, or at the international level.[1886] However, in three of the EU Copyright Directives, originality has been defined as the "author's own intellectual creation".[1887] Such a standard was also adopted by the CJEU in the *Infopaq* decision when interpreting the notion of work under the Information Society Directive,[1888] and has been subsequently restated in a number of rulings.[1889] This interpretation and expansion has been the object of well-

1884 *Coco v A.N.Clark (Engineers) Ltd* [1969] RPC (Ch).

1885 See chapter 5 § 3 A).

1886 Elizabeth F. Judge and Daniel Gervais, 'Of Silos and Constellations: Comparing notions of Originality in Copyright Law' [2009] 27 Cardozo Arts and Entertainment LJ 375, 377 distinguish between four families of standards in copyright law: (i) the EU's "author own intellectual creation"; (ii) the US "minimal degree of creativity"; (iii) the Canadian "non-mechanical and non-trivial exercise of skill and knowledge" and (iv) the UK's "skill and labor".

1887 Database Directive (Article 3(1)), Software Directive (Article 1(3)); Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights (codified version) [2006] OJ L372/12 (Term of Protection Directive), (Article 6).

1888 In Case C–5/08 *Infopaq International v Danske Dagblades Forening* [2009] ECR I-6569, paras 37-39 the CJEU ruled that: "copyright within the meaning of Article 2(a) of Directive 2001/29 is liable to apply only in relation to a subject matter which is original in the sense that it is its *author's own intellectual creation*. (…) The various parts of a work thus enjoy protection under Article 2(a) of Directive 2001/29, provided that they contain elements which are the *expression of the intellectual creation of the author of the work*" (emphasis added).

1889 See Case C–5/08 *Infopaq International v Danske Dagblades Forening* [2009] ECR I-6569 para 37 and subsequent decisions from the CJEU: Case C–393/09 *Bezpečnostní softwarová asociace v Ministerstvo kultury* [2010] ECR I-13971, para 45; Joined Cases C-403/08 and C-429/08 *Football Association Premier League and Others* [2011] ECR I-9083, para 97; Case C–145/10 *Eva-Maria Painer v Standard VerlagsGmbH and Others* [2011] ECR I-12533, para 87 and Case C–604/10 *Football Dataco Ltd and others v Yahoo! UK Ltd and others* (CJEU, 1 March 2012) paras 37-47; a more detailed analysis of the harmonisation of the notion of originality through the case law of the CJEU falls outside the scope of the present research; however a more comprehensive account is provided by Gernot Schulze, 'Schleichende Harmonisierung des urheberrechtlichen Werkbe-

founded criticism by legal academia, both from an intellectual property and a constitutional perspective, particularly in the UK, where the threshold of originality was comparatively lower than in continental Europe.[1890] In effect, traditionally, the English concept of originality was intended to protect works resulting from the "labour, skill or judgement" invested in creating them.[1891] In contrast, the concept of an author's own intellectual creation sets a higher bar, as following the traditional French test a work must be an expression of the author's personality.[1892]

In the context of trade secrets, the originality requirement, like the novelty prong, has been discussed in particular with regard to the entertainment and manufacturing industries, where an idea with potential to be exploited is imparted to a third party, who ends up developing and exploiting it in a commercial manner.[1893] The following sections look into how courts in the U.S. and England have construed such a requirement.

1. U.S.

In the U.S., a number of cases have noted that the information protected by a trade secret should present a certain degree of "originality". By way of illustration, in *Cataphote Corporation v. Hudson*,[1894] the Court of Appeals of the Fifth Circuit deemed that the techniques and processes to manufacture glass beads used by a former employee of the plaintiff that went on to create a competing firm were not protectable as a trade secret because in order to be protected, information "must possess at least that modicum of originality which will separate it from everyday knowledge".[1895] Following the same legal reasoning as the U.S. cases examined above with respect to

griffs? - Anmerkung zu EuGH "Infopaq/DDF"' [2009] GRUR 1019 and Silke von Lewinski, 'Introduction: The Notion of Work under EU Law' [2014] GRUR Int 1098.

1890 Eleonora Rosati, 'Originality in a work, or a work of originality: the effects of the Infopaq decision' [2011] 33 EIPR 746-755.

1891 *Ladbroke v William Hill* [1964] 1 WLR 273, 278.

1892 Elizabeth F. Judge and Daniel Gervais 2009 (n 1886) 386 note that two interpretations of the expression of an "author's own intellectual creation" are possible: (i) as a form of expressing the personhood of the author and (ii) as noting the absence of copying by the author.

1893 James Pooley 2002 (n 66) § 4.03[3] 4-21- 4-22.

1894 *Cataphote Corporation v. Hudson*, 444 F.2F 1313 (5th Cir. 1971).

1895 *Cataphote Corporation v. Hudson*, 444 F.2F 1313, 1315 (5th Cir. 1971).

the novelty requirement,[1896] the court concluded that an idea or process that is common, well known or readily ascertainable "lacks all novelty, uniqueness and originality, it necessarily lacks the element of privacy necessary to make it legally cognizable as a trade secret".[1897]

2. England

In England, one of the leading cases on the originality requirement within the breach of confidence action is *De Maudsley v Palumbo.*[1898] In short, the facts of the case are as follows: the plaintiff (Mr Maudsley) came up with the idea of opening a night club in London with the particularity that it could be legally open all night long and have sound equipment of the highest quality. He disclosed this idea to the defendant, Mr Palumbo, during the course of a party. A year later, the defendant opened a club, the world famous Ministry of Sound, with those same features. As a result, Mr Maudsley brought an action against Mr Palumbo for breach of confidence. In delivering the judgement, the court dismissed the action, establishing that for a literary, creative or entertainment industry idea to achieve the status of confidential information it: "(1) must contain some significant element of originality, (2) be clearly identifiable (as an idea of the confider), (3) be of potential commercial attractiveness, and (4) be sufficiently well developed to be capable of actual realisation".[1899] As regards the latter requirement, the court went on to argue that "before the status of confidential information can be achieved by a concept or idea it is necessary to have gone far from identifying a desirable goal. A *considerable degree of particularity in a definite product* needs to be shown to be the result of a mental process in question" (emphasis added).[1900]

The protectability of an idea for a new television series was also litigated before English courts, but with a different outcome than in the U.S. case *Murray v. National Broadcasting Company*[1901] examined above.[1902] In *Fraser v Thames Television Ltd*[1903] the possibility of relying on the breach of confi-

1896 See chapter 4 § 4 E) I. 2. a).
1897 *Cataphote Corporation v. Hudson*, 444 F.2F 1313, 1315 -1316 (5th Cir. 1971).
1898 *De Maudsley v Palumbo* [1996] FSR 447 (Ch).
1899 *De Maudsley v Palumbo* [1996] FSR 447 (Ch), 448.
1900 *De Maudsley v Palumbo* [1996] FSR 447 (Ch), 465.
1901 *Murray v. National Broadcasting Co., Inc.,* 844 F.2.d 988 (2d Cir. 1988).
1902 Chapter 4 § 4 E) I. 2. a).
1903 *Fraser v Thames Television Ltd* [1984] QB 44 (QB).

dence action to protect an idea for a television series about the actual experiences of three females members of a rock group was evaluated. The idea for such a series was first developed by the manager of a pre-existing three rock-girl group ("Rock Bottom"), who submitted it for consideration to a screenwriter, a television company ("Thames") and a producer (the "defendants"). During the initial negotiations, it was agreed that the three members of the band would act as the main characters of the series and that the information had been disclosed in confidence. However, the negotiations ultimately broke off and after some months, Thames, along with the other two defendants, produced a series based largely on the idea submitted by the plaintiffs, who sought damages for an alleged breach of confidence.[1904]

In its legal reasoning the court started by noting that ideas communicated orally were eligible for protection under the breach of confidence action, provided that the other requirements were met.[1905] In this regard, it further stated that to merit protection ideas must present an element of "originality", which may consist of a significant "twist or slant" on a well-known concept.[1906] Indeed, such a requirement correlates with the novelty requirement demanded in industrial settings.[1907] Against this background, it was ruled that to be protected ideas must be imparted in confidence and their content must be "(i) *clearly identifiable*, (ii) *original*, (iii) of *potential commercial attractiveness* and (iv) *capable of being realised in actuality*".[1908]

The fourth requirement has garnered substantial attention and was examined by the High Court of England in 2005 in a decision concerning the alleged misappropriation of design ideas for a cone-shaped device with a triple spiral to treat water (*Sales v Stromberg*[1909]). The court held that the idea of a triple spiral design was not protectable because it was not capable of being "put into practice in a practical way".[1910]

III. Conclusion – protection of abstract ideas

As is apparent from the comparative analysis conducted in the previous sections, courts have applied the requirements of novelty and originality to

1904 *Fraser v Thames Television Ltd* [1984] QB 44 (QB).
1905 *Fraser v Thames Television Ltd* [1984] QB 44 (QB), 65.
1906 *Fraser v Thames Television Ltd* [1984] QB 44 (QB), 65.
1907 *Fraser v Thames Television Ltd* [1984] QB 44 (QB), 65.
1908 *Fraser v Thames Television Ltd* [1984] QB 4, 66.
1909 *Sales v Stromberg* [2006] FSR 7 (Ch).
1910 *Sales v Stromberg* [2006] FSR 7 (Ch), 111.

avoid the privatising of information already in the public domain based on trade secrets misappropriation claims. Indeed, a review of the relevant case law in the U.S. and England reveals that when courts require information to be novel or original they are ultimately enquiring into whether the information is secret or easily accessible, either because the information is in fact well-known among industry members (or even the general public) or because it is an evident variation of an existing technical solution. Consequently, it is submitted here that the novelty and originality enquiries do not constitute separate requirements of protection, but are in in fact subsumed within the general secrecy assessment. Therefore, in view of the harmonisation goals pursued by the TSD, it is advisable that courts across the EU refrain from using such terminology and confine their assessment to whether the information is in fact generally known or easily accessible.

In the same vein, the analysis of the case law examined above has underscored that courts on both sides of the Atlantic Ocean have struggled to draw a line between ideas in the public domain and those that should be afforded protection under the trade secrets regime in the U.S. and under the breach of confidence action in England. Indeed, in the U.S. this has given rise to a separate body of case law known as the "law of ideas" based on a number of legal doctrines; the contours of this remain sketchy and it has been criticised for its highly disruptive effects within the intellectual property legal system.[1911] As argued in chapter 1, abstract ideas do not merit protection either from the intellectual property regime perspective or from an unfair competition standpoint,[1912] and the same principle should be applied to the trade secrets legal regime. However, establishing when the level of abstraction is such that it precludes the privatisation of information runs as a common threat among all intellectual property doctrines.[1913]

In the light of the above, the better view it is submitted, is that courts should assess whether a specific idea imparted to a third party qualifies for protection as a trade secret by reference to the general three-step test enshrined in Article 2(1) TSD:

(i) The first step requires that information is not generally known or easily accessible. Abstract ideas will usually be devoid of such a concealed nature as no effort, skill or labour will be necessary to develop them. In the same vein, obvious variations of information in the public do-

1911 Melville B. Nimmer 1954 (n 1866) 140-144.
1912 See chapter 1 § 3 B) I.
1913 See chapter 1 § 3 B) II.

main should be considered as easily accessible and therefore not protectable either. Only more elaborate ideas developed after the investment of substantial labour, effort and intellectual skill will merit protection.

(ii) According to the second prong of the definition, ideas should only merit protection if they have commercial value (actual or potential) due to their undisclosed nature. In the context of ideas submitted for consideration to a third party, such a requirement should be understood as demanding that ideas present potential commercial attractiveness ("some kind of commercial twist").

(iii) The third limb of the definition requires that information is subject to reasonable steps under the circumstances to maintain its secret nature. This thesis has argued in favour of interpreting this requirement as a rather low threshold. In particular, as regards the protection of ideas, it will suffice that the parties execute an NDA, or that such a duty can be implied from the relationship between the parties (for example, between employer and employee).

(iv) As a final note, and in line with the arguments submitted in the present chapter,[1914] it is of utmost importance that the idea for which protection is sought is identified in a precise manner. Even though this may seem evident, it is essential to achieve an optimal equilibrium between the private sphere of a company and the public domain. In addition, it should further be required that such ideas are capable of being realised (put into practice), in other words, capable of being developed into a "finished product", in line with the English case law examined.[1915]

In sum, it appears that the more detailed and elaborate an idea is, the more likely it is to be afforded protection by courts. By way of illustration, the disclosure of a general idea for a television series that portrays a black family in a non-stereotypical manner (such as in the *Murray v. National Broadcasting Company* case)[1916] is unlikely to qualify for protection, because it falls short of the secrecy requirement. In turn, its inherent abstract nature will also substantially deprive the idea of commercial attractiveness, as commercial twists usually arise with regard to more developed concepts.

1914 See chapter 4 § 3 F).

1915 John Hull 1998 (1016) paras 3.64-3.65.
De Maudsley v Palumbo [1996] FSR 447 (Ch), 469; more recently, *Sales v Stromberg* [2006] FSR 7 (Ch).

1916 *Murray v. National Broadcasting Co., Inc.*, 844 F.2.d 988 (2d Cir. 1988).

However, if the idea were to be developed further and presented to a TV network or a producing company in the format of a TV Bible[1917] that subsequently went on to produce it following the guidelines outlined in the Bible without authorisation from the originator (and without paying appropriate consideration), courts would be more likely to grant relief. Indeed, similar considerations were followed by the Queen's Bench Division of the High Court of England and Wales in *Fraser v Thames Television Lt.*[1918] After all, from a practical perspective, if the information is recorded in a physical support, plaintiffs will be able to define the object of protection in a much more precise manner and thereby provide more convincing evidence of the alleged misappropriation.

More generally and from a policy perspective, it seems unsound to impose qualitative restrictions on the type of information protected under the trade secrets legal regime, since these are already embedded in the IPRs system and may conflict with the balance struck by the latter. As examined throughout this dissertation, trade secrets, unlike IPRs, do not confer erga omnes rights on their holders. They only afford protection against misappropriation and may not be enforced against third parties outside of the confidential relationship if the information is acquired by lawful means.

F) Excursus: Trade secrets and Big Data — the way forward?

The emergence of the Data Economy has brought along a drastic shift in the use of data paradigm, as data have now become a key asset for innovation and economic growth.[1919] The inherent technical complexity of the phenomena that have arisen in this new context has given rise to numerous questions regarding the legal framework applicable to the newest data markets. Consequently, as outlined above,[1920] the Commission is contemplating several potential regulatory options in the context of the "Building

1917 A document used by producers and screenwriters in which the characters, the settings and the plot are explained in detail.

1918 *Fraser v Thames Television Ltd* [1984] QB 44.

1919 Josef Drexl 2016 (n 426) 9; OECD, 'Data-Driven Innovation: Big Data for Growth and Well-Being' (OECD Publishing 2015) 11-15 <http://dx.doi.org/10.1787/9789264229358-en> accessed 15 September 2018.

1920 See chapter 1 § 3 B) II. 4.

a European Data Economy Initiative".[1921] The Synopsis Report of the Consultation launched by the Commission indicated that stakeholders mostly regard that the TSD and the Database Directive already provide the most adequate framework for the protection of Big Data.[1922] Notwithstanding this, from a theoretical perspective, the application of the trade secrets legal regime to Big Data sets raises many interpretative questions.[1923] Before turning to them, it is necessary to provide some clarification regarding the functioning of the Data Economy and the concepts that are most frequently used in connection with it (section I). This is essential in order to provide a better understanding of the intersection between Big Data and the law of trade secrets, which is analysed under section II.

I. The Data Economy and the associated phenomena

The Commission has defined the Data Economy as "an ecosystem of different types of market players -such as manufacturers, researchers and infrastructure providers- collaborating to ensure that data is accessible and usable".[1924] In such a dynamic ecosystem, new business models that are fundamentally different to the business models that dominated the web 2.0 landscape (search engines and social networks) have emerged. In the web 2.0 environment, search engines and social networks used the personal data of their users to provide them with personalised advertisements, thereby financing the provision of their services.[1925] By contrast, nowadays data

1921 Commission, 'Building a European Data Economy Initiative' COM(2017) 9 final.

1922 Commission, 'Synopsis Report on the Consultation on the Building a European Data Economy Initiative.' (2018) 5 <https://ec.europa.eu/digital-single-market/en/news/synopsis-report-public-consultation-building-european-data-economy> accessed 15 September 2018.

1923 The application of the sui generis database right to protect Big Data sets also appears problematic, as outlined in chapter 1 § 3 A) IV. 2. However, providing an in depth-study of this topic falls outside the scope of the present research.

1924 Commission, 'Building a European Data Economy Initiative' COM(2017) 9 final, 2.

1925 Josef Drexl 2016 (n 426) 8-9 describes the three stages of development of the Internet: "At this first stage of development the Internet emerged as an information and selling platform (web 1.0). At the second stage, new business models developed that provided consumers with other kinds of services, yet still related to information, without charging them a price. These services, such as search engines or social platforms that connect people with people (web 2.0),

have become an *infrastructural resource* that can be used to create products and services for an unlimited number of purposes and in a non-rivalrous manner[1926] and, consequently, they are viewed as a valuable driver for innovation.[1927] Indeed, in the Data Economy, data analytics have turned out to be increasingly important as value creation mechanisms, mainly for two reasons: (i) on the one hand, they allow for gaining knowledge and control over the analysed objects, for example, environmental phenomena; and (ii) on the other hand, they automate decision-making processes with the use of autonomous machines, as illustrated by autonomous vehicles.[1928]

In this new ecosystem, new technologies have arisen allowing for the connectivity of machines and systems. These phenomena have been grouped together under the more general concept of the IoT, which essentially consists of "adding sensors and Internet capability to everyday physical objects",[1929] such as cars, lamp posts and refrigerators, to name some. The combination of those elements and the performance of data analysis ultimately lead to machine learning and remote control and allow for the development of autonomous machines and systems. Consequently, in recent years, the development of smart products and services has increased exponentially.[1930]

---

were often exclusively financed by advertising. Whereas at the first stage, information was largely limited to information as an object of the service, at the second stage personal data became a most important input for new kinds of business models that were information related. The advertising value of a service or platform increases with its attractiveness for private users who, in turn, provide its operator with personal data as the key input for such business models"; see further Amir Gandomi and Murtaza Haider, 'Beyond the hype: Big data concepts, methods, and analytics' [2015] 35 International J of Information Management 137, 142.

1926 OECD, 'Data-Driven Innovation: Big Data for Growth and Well-Being' (OECD Publishing 2015) 4 <http://dx.doi.org/10.1787/9789264229358-en> accessed 15 September 2018.

1927 Wolfgang Kerber 2016 (n 446) 989.

1928 OECD, 'Data-Driven Innovation: Big Data for Growth and Well-Being' (OECD Publishing 2015) 4 <http://dx.doi.org/10.1787/9789264229358-en> accessed 15 September 2018.

1929 The Economist, 'Where the smart is' (San Francisco, 11 June 2016) <https://www.economist.com/news/business/21700380-connected-homes-will-take-longer-materialise-expected-where-smart> accessed 15 September 2018.

1930 Bart van der Sloot and Sascha van Schendel, 'Ten Questions for Future Regulation of Big Data: A comparative and Empirical Legal Study' [2016] 7 JIPITEC 110 paras 16-17.

This new complex scenario is best explained through a real example case, such as the networked car.[1931] In June 2017 Volkswagen released a press statement announcing that as of 2019 some of its models would incorporate the "pWLAN" standard, which enables direct communication between vehicles, as well as transport infrastructure and international markets.[1932] The implementation of such a technology will allow for sharing real-time information gathered by the numerous sensors included in the cars on the state of the traffic, accidents and even environmental conditions within a radius of 500 metres, without the need to rely on a mobile network. It further aims at providing greater safety and traffic efficiency, helping users to avoid risky situations. The statement concludes by noting that the effectiveness of the pWLAN technology will improve with use, thereby highlighting the network effects of data sharing in the Data Economy. As a result, the note issued by Volkswagen also emphasises that the company is working together with other car manufacturers, industry partners, as well as public authorities in order to spread the inclusion of the pWLAN technology in serial production.[1933]

The big streams of data collected by tracking the activities of consumers that browse the web or by sensors incorporated into physical interconnected objects, such as in the case of the networked car outlined above, are subsequently included in larger datasets for their management and analysis.[1934] These datasets are generally referred to as "Big Data", alluding to one of the defining features of the collections of data in the Digital Economy: their sheer magnitude.[1935] However, conceptualising the Big Data phenomenon solely by reference to this parameter appears over-simplistic. Indeed, the most frequently cited definition refers to a confluence of factors, the so-called "three V's":

1931 This is the example propposed by Andreas Wiebe 2016 (n 287) 878.

1932 Volkswagen, 'With the aim of increasing safety in road traffic, Volkswagen will enable vehicles to communicate with each other as from 2019' (28 June 2017) <https://www.volkswagen-media-services.com/en/detailpage/-/detail/With-the-aim-of-increasing-safety-in-road-traffic-Volkswagen-will-enable-vehicles-to-communicate-with-each-other-as-from-2019/view/5234247/7a5bbec13158edd433c6630f5ac445da> accessed 15 September 2018.

1933 Ibid.

1934 Amir Gandomi and Murtaza Haider 2015 (n 1925) 139-140.

1935 OECD, 'Data-Driven Innovation: Big Data for Growth and Well-Being' (OECD Publishing 2015) 11 <http://dx.doi.org/10.1787/9789264229358-en> accessed 15 September 2018.

i. *Volume* alludes to the dimension of the datasets, which are measured in terabytes and petabytes.[1936]
ii. *Variety* refers to the heterogeneity of the data sources, which may be structured, but most frequently are not.[1937] Data may be obtained from a myriad of sources ranging from social media or web blogs to financial communications and sensors incorporated into physical objects.[1938] The term variety also refers to the possibility of establishing a correlation between the different data sources.[1939]
iii. *Velocity* highlights the rate at which data are generated, accessed and processed.[1940] The predictive power of data analytics is higher than ever before, allowing companies to use it in a much more precise way.[1941]

In addition to the three above-mentioned variables, it has been suggested that there are further features that are usually deployed in the common framework for characterising Big Data, namely:

iv. *Value*, which underscores that Big Data presents "low value density". That is, individual data bits as such may have little value, yet upon analysis of large amounts of collected data it is possible to obtain substantial value.[1942]

1936 Mike Loukides, 'What is Data Science?' (2010) <https://www.oreilly.com/ideas/what-is-data-science> accessed 15 September 2018; Amir Gandomi and Murtaza Haider 2015 (n 1930) 138.
1937 Amir Gandomi and Murtaza Haider 2015 (n 1925) 138.
1938 These are just some of the examples outlined in OECD, 'Data-Driven Innovation: Big Data for Growth and Well-Being' (OECD Publishing 2015), 14 <http://dx.doi.org/10.1787/9789264229358-en> accessed 15 September 2018.
1939 Federal Trade Commission, 'Big Data: A Tool for Inclusion or Exclusion, Understanding the issues' (2016) FTC Report, 1 <https://www.ftc.gov/reports/big-data-tool-inclusion-or-exclusion-understanding-issues-ftc-report> accessed 15 September 2018.
1940 Amir Gandomi and Murtaza Heider 2015 (n 1925) 138.
1941 Federal Trade Commission, 'Big Data: A Tool for Inclusion or Exclusion, Understanding the issues' (2016) FTC Report, 2 <https://www.ftc.gov/reports/big-data-tool-inclusion-or-exclusion-understanding-issues-ftc-report> accessed 15 September 2018.
1942 Richard Winter, 'Big Data: Business Opportunities, Requirements and Oracle's Approach' (2011) Executive Report, 2 <http://www.oracle.com/us/corporate/analystreports/infrastructure/winter-big-data-1438533.pdf.> accessed 15 September 2018.

v. *Veracity*, which refers to the unprecise and uncertain nature of the data collected, for example, when it comes to measuring customers' sentiments.[1943]
vi. *Variability and complexity*, which emphasises that data fluctuation is a common phenomenon and that individual data are obtained from multiple sources.[1944]

Notwithstanding the aforementioned, defining Big Data solely by reference to the confluence of factors spelt out above has been criticised for not signalling the different ends for which data can be used, as well as for the fact that the full potential of data is only unlocked after the large streams of individual data bits are processed and analysed.[1945] The importance of data analytics as value creation mechanisms was stressed by the Federal Trade Commission ("FTC") in a report in which the legal issues surrounding the emergence of the Big Data phenomena in the U.S. were discussed.[1946] According to the FTC, the life cycle of Big Data is divided into the following four stages: (i) collection, (ii) compilation and consolidation, (iii) data mining and analytics,[1947] and (iv) use.[1948] In the first stage of the

1943 Amir Gandomi and Murtaza Heider 2015 (n 1925) 138.
1944 Amir Gandomi and Murtaza Heider 2015 (n 1925) 137.
1945 OECD, 'Data-Driven Innovation: Big Data for Growth and Well-Being' (OECD Publishing 2015) 30 <http://dx.doi.org/10.1787/9789264229358-en> accessed 15 September 2018; Amir Gandomi and Murtaza Heider 2015 (n 1925) 139-140 note that "Big data are worthless in a vacuum. Its potential value is unlocked only when leveraged to drive decision making. To enable such evidence-based decision making, organizations need efficient processes to turn high volume of fast-moving data into meaningful insights".
1946 Federal Trade Commission, 'Big Data: A Tool for Inclusion or Exclusion, Understanding the issues' (2016) FTC Report, 3-4 <https://www.ftc.gov/reports/big-data-tool-inclusion-or-exclusion-understanding-issues-ftc-report> accessed 15 September 2018.
1947 A detailed account of the current trends and perspectives of data analytics see Karthik Kambatla, Giorgos Kollias, Vipin Kumar and Ananth Grama, 'Trends in big data analytics' [2014] 74 J of Parallel and Distributed Computing 2561-2573.
1948 Federal Trade Commission, 'Big Data: A Tool for Inclusion or Exclusion, Understanding the issues' (2016) FTC Report 3-4; in a similar vein see Herbert Zech, 'Data as Tradeable Commodity – Implications for Contract Law' 2 in Josef Drexl (ed), *Proceedings of the 18th EIPIN Congress: The New Data Economy between Data Ownership, Privacy and Safeguarding Competition* (Edward Elgar) (forthcoming) notes that the Data Economy is divided into four sequential stages: (i) production of data; (ii) collection of data; (iii) analysis of data and (iv) possible innovations resulting from the analysis <https://ssrn.com/abstract=3063153> accessed 15 September 2018.

value chain, data are gathered from a variety of sources, such as tracking cookies or interconnected sensors incorporated into physical devices (IoT). Next, the raw data are systematised by entities such as online ad networks, social media companies, online platforms or data aggregation entities.[1949] Crucially, during the third stage, the data are analysed in order to unveil common patterns or other characteristics across the compiled datasets. In recent years, the emergence of predictive data analytics techniques has allowed firms to anticipate new or future observations i.e. to create new data on the basis of pre-existing data sets.[1950] In effect, in the value chain of Big Data, data-based innovations can only take place after the collection of data.[1951] In the latter stage, the insights obtained from the previous phases are used in the context of process optimisation.

The complex flow of data and the multiple stakeholders that take part in the value networks[1952] that operate in the Data Economy have given rise to a high level of legal uncertainty regarding the ownership and access to data conditions.[1953] For instance, following the networked car example mentioned above, several stakeholders may have an interest in the information collected by the sensors and mobile applications incorporated in smart vehicles, including the car owner and the user, as well as navigation service providers, who may be able to improve the quality of their services through real-time analysis of the gathered data.[1954] Similarly, insurance companies may find such information useful to provide individualised

1949 Federal Trade Commission, 'Big Data: A Tool for Inclusion or Exclusion, Understanding the issues' (2016) FTC Report, 3-4 <https://www.ftc.gov/reports/big-data-tool-inclusion-or-exclusion-understanding-issues-ftc-report> accessed 15 September 2018.

1950 As noted by Galit Shmueli, 'To Explain or to Predict?' [2010] 25 Statistical Science 289, 291.

1951 Herbert Zech 2016 (n 278) 58.

1952 In this context, Josef Drexl 2016 (n 426) 16-17 underscores that in the "traditional economy" the value creation paradigm is of a vertical nature, where "manufacturers purchase input for the production of goods in upstream markets and then sell them through distribution chains – often including wholesales and distributors- to consumers. At each level of the production and distribution chain, some economic value is added". By contrast, in the Data Economy, value enlarges through value networks.

1953 As suggested by Andreas Wiebe 2016 (n 287) 878.

1954 See Wolfgang Kerber 2016 (n 446) 995; more generally the OECD, 'Data-Driven Innovation: Big Data for Growth and Well-Being' (OECD Publishing 2015) 14 <http://dx.doi.org/10.1787/9789264229358-en> accessed 15 September 2018 identified the following six key types of players: "(i) Internet service providers providing the backbone of the data ecosystem, (ii) IT infrastructure providers

prices to their customers based on the analysis of real-time risk and their behaviour while driving.[1955] Governmental authorities could also benefit from access to such data, as they would be able to gain an insight into the state of the traffic, or use it in managing toll systems or in crime prevention.[1956] Finally, Internet Service Providers ("ISPs") may also be interested in such data, which may allow them to provide targeted advertisements. Notably, as stressed by Drexl, a distinctive characteristic of the Data Economy is the "increasing role of Internet Intermediaries" on the basis of a twofold rationale: (i) ISPs are aware of the consumer preferences and control data interfaces, and consequently (ii) they are at a competitive advantage in the penetration of the smart products markets.[1957]

---

offering data management tools and critical computing resources including, but not limited to, data storage servers, database management software, and cloud computing resources, (iii) data analytic providers who supply software solution for data analysis including data visualisation, (iv) data providers, mainly the consumers (…), (v) governments through their open data initiatives (…), firms such as in particular data brokers and data market places (…), and increasingly owners of interconnected machines and systems (…), and last but not least (vi) data-driven entrepreneurs, who build their innovation on top of the resources provided in the data ecosystem in areas such as retail, finance, advertisement, science (…) and health (…) to name a few".

1955 'Huge volumes of data make real time insurance a possibility – Pay per risk' *The Economist* (21 September 2017) <https://www.economist.com/finance-and-economics/2017/09/21/huge-volumes-of-data-make-real-time-insurance-a-possibility> accessed 15 September 2018: "Conventional insurance works by pooling individual risks and then setting a price for that group- new drivers under 30, say. But the process can be much refined if the objects and people being insured can report to the insurer automatically, and if there is a wealth of data on the external environment. As an ever-growing number of sensors- in phones or watches, drones or cars – gathers ever-greater volumes of data, more and more activities can be assessed for real-time risk (though in the absence of pooling, some risks may become prohibitely expensive to insure)".

1956 Andreas Wiebe 2016 (n 287) 879.

1957 From a competition law perspective, Josef Drexl 2016 (n 426) 17-18 further indicates that "whereas the digital transformation of the industry decreases existing entry barriers and may even force industrial incumbents out of the market, control over data enables firms originating in the Internet sector, such as Google, to enter into and gain considerable market power in a large variety of different markets for the production and operation of smart products. Recognition of data ownership may therefore have the unwanted effect of strengthening the market power of these firms even more, while, from a competitive perspective, it would be wiser to promote access to data that is needed by other market players to operate in such markets".

In the context of the myriad of potential stakeholders that may have an interest in accessing the data created in the Data Economy environment, the most salient legal issue that arises is whether any of the applicable existing legal regimes may afford protection to industrial data or instead whether exclusivity should be granted over the said data at the collection level by the introduction of a sui generis right (prior to any innovations).[1958] As noted above,[1959] this prompted the Commission to launch a consultation in order to assess, among other options, the possibility of introducing a "data producers' right" over industrial data, as there seems to be consensus regarding the fact that industrial data, as such, are not protected by any exclusive intellectual property right.[1960] However, existing regimes such as contract law, criminal law, tort law or trade secrets may already provide a robust legal framework for industrial data governance.[1961] Providing an in-depth analysis of such a complex topic falls outside the scope of this dissertation. Thus, this thesis is confined to the study of the possibility of relying on the trade secrets legal regime for the protection of industrial data (section 2).

II. Assessing the possibility of relying on trade secrets protection for industrial data

As noted in chapter 1, the TRIPs Agreement defines trade secrets as undisclosed information.[1962] Following the theory of semiotics, trade secrets protect information at the semantic level, i.e. information with a specific

---

1958 Herbert Zech 2016 (n 278) 58.

1959 Chapter 1 § 3 B) II. 5.

1960 Commission, 'Commission Staff Working Document on the free flow of data and emerging issues of the European data economy' SWD(2017) 2 final, 19 concluded that "Machine-generated and industrial data do not benefit from protection by other intellectual property rights as they are deemed not to be the result of an intellectual effort. Results of data integration, analytics, etc. can be protected, on the other hand, as a result of a protection given to the intellectual effort made into the design of the data integration process or the analytics algorithm (software)"; an overview of the academic debate is provided by Andreas Wiebe 2016 (n 287) 880; Josef Drexl and others 2017 (n 442) paras 9-17; Josef Drexl 2016 (n 426) 19-26, Michael Dorner, 'Big Data und "Dateneigentum"' [2014] CR 617, 622; Josef Drexl and others 2017 (n 442) paras 9-17.

1961 See Wolfgang Kerber 2016 (n 446) 998.

1962 See chapter 2 § 1 A) IV.

meaning.[1963] Hence, at first glance, industrial data and the algorithms used to create them seem to fall within the scope of protection of trade secrets, both according to the minimum standards set out in the TRIPs Agreement and the harmonised legal regime introduced by virtue of the TSD. However, upon closer examination, the technical specificities of Big Data and the survey of the requirements of protection that trigger liability under the TSD call for a more nuanced approach, which is analysed under section (1). Indeed, several legal scholars have criticised the TSD, stating that it was out of date even before its implementation deadline, because the European legislator overlooked its potential applicability in the Data Economy.[1964] Next, additional issues in the application of the TSD to the protection of Big Data are outlined (section 2), from which conclusions are drawn (section 3).

1. Reconciling the legal requirements of protection of trade secrets law with Big Data

According to the TRIPs Agreement and the TSD,[1965] information can be protected so long as: (i) it is "secret" in the sense that it is not "generally known among or readily accessible to persons within the circles that normally deal with the information in question"; (ii) it has commercial value due to its secret nature; and (iii) it has been subject to reasonable steps under the circumstances to maintain its concealed nature. The applicability of these three requirements to the large streams of data that are gathered and analysed in the context of Big Data requires specific consideration.

As regards the first requirement, it should be noted that one of the defining features of the Data Economy is the ubiquity of data collection, which allows different physical objects equipped with sensors connected to the IoT to gather the same data. Consequently, it has been argued that if the individual data can be simultaneously collected by different sensors and machines, the secrecy requirement will not be satisfied.[1966] The networked car example illustrates this in the most clear manner: if several vehicles collect the same information on the state of transit and transfer it to

1963 Herbert Zech 2015 (n 423) para 8.
1964 This is noted by Andreas Wiebe 2016 (n 287) 880; similarly Josef Drexl 2016 (n 426) 22.
1965 See Article 39(2) TRIPs, Article 2(1) TSD.
1966 Josef Drexl 2016 (n 426) 23.

different car manufacturers, the individual data will be deemed generally available, thus forfeiting trade secrets protection.

However, it cannot be affirmed from the outset that Big Data sets should be automatically regarded as publicly known. On both sides of the Atlantic, namely, the U.S., Germany and England, courts have construed the secrecy requirement as comprising the assembly of elements in the public domain when it results in a separate secret entity, a so-called "combination secret".[1967] This is the rationale that is usually followed with regard to the protection of customer lists, which are mostly made up of information that is publicly available, but are nonetheless deemed eligible for protection in most jurisdictions, provided that the lists as a discrete entity are not available to competitors.[1968]

Against this background, the analytical framework proposed above in the context of combination secrets appears of utmost relevance in assessing the protection of Big Data sets under the harmonised framework created by the TSD.[1969]

Pursuant to the first factor, the gathering of individual data that can be simultaneously collected by competitors will still be eligible for protection if there is a functional interrelationship between the elements in the claimed combination secret. In the context of Big Data, such a requirement is easily met, as the individual data are integrated into larger sets following a unified process.

The second factor purports that the combined elements should have more value than the individual elements considered in isolation. The application of this factor allows for overcoming the definitional problems raised by the commercial value requirement, as it has been suggested that individual data on ephemeral events as such may not fulfil this condition. In effect, in the Data Economy, the full potential of data is only unlocked after a data analytics process. In this context, the wording of Recital 14 of the TSD appears to be particularly relevant.[1970] On the one hand, it expressly clarifies that the value of data can be both "actual" and "potential",

---

1967 Chapter 4 § 4 C) II. 5.

1968 Gintare Surblyte 2016 (n 281) 11-12.

1969 Chapter 4 § 4 C) II. 5. d)

1970 See Recital 14 of the TSD: "(...) Furthermore, such know- how or information should have a commercial value, whether *actual* or *potential*. Such know-how or information should be considered to have a commercial value, for example, where its unlawful acquisition, use or disclosure is likely to harm the interests of the person lawfully controlling it, in that it undermines that person's scientific and technical potential, business or financial interests, strategic positions

which seems to indicate that individual data may be eligible for protection if, from their inclusion in larger data sets and subsequent analysis, it is possible to obtain insights that reveal common patterns or any other valuable information. On the other hand, it further indicates that "trivial information" shall not qualify for protection under the law of trade secrets. This apparent tension can be solved most effectively through the application of the methodology of statutory legal interpretation. From a semantic perspective, *trivial* is an adjective that is used to refer to items of "little value or importance".[1971] However, following a systematic interpretation of the provisions of the TSD, the exclusion of trivial information should not extend to individual data that are included in larger datasets for their subsequent analysis. Indeed, such individual data should be considered to have, at least, potential value and therefore be eligible for protection under the definition of trade secrets provided in Article 2(1) of the TSD.[1972] Their value lies in their incorporation in big data sets. Yet, in practice, establishing such a causality relationship may prove very complex for the trade secret holder.[1973]

The third factor enquires into whether the combination resulted from the investment of "intellectual skill", assessed against the existing alternatives used by the members of the relevant circles. At first glance, this principle may not appear applicable to Big Data sets, as they are mostly gathered automatically. However, it is submitted that this prong should be construed as referring to the intellectual investment in the development of the collection, processing and analysing mechanisms (mostly algorithms and code) developed by the trade secret holder. If these are known or easily accessible among the industry members (for instance, if several metasearch engines use the same sources of data and the same pre-existing scrapping program, which is furthermore well-known within an industry), the Big Data sets should not qualify for trade secrets protection, as they will not confer any competitive advantage over the existing alternatives.

Additionally, it is submitted that in the enforcement of trade secrets protection against the misappropriation of Big Data sets, courts should take into consideration whether the competitor generated the data indepen-

---

or ability to compete. The definition of trade secret excludes *trivial* information (...)"(emphasis added).

1971 'trivial, adj' (*OED Online*, OUP June 2013) <https://en.oxforddictionaries.com/definition/trivial> accessed 15 September 2018.

1972 Andreas Wiebe 2016 (n 287) 880 suggests that there may no longer be trivial information.

1973 Josef Drexl 2016 (n 426) 23.

dently or acquired it through reverse engineering (factor 4), and should demand that the plaintiff identify precisely the information concerned (factor 5). However, the latter appears rather complex in view of the sheer volume of Big Data sets and the pace at which they develop. Big Data sets are dynamic in nature.

From a practical point of view, it should be noted that technological measures that prevent the unauthorised access of third parties to the content of Big Data sets may allow data holders to achieve *de facto* exclusivity over them. In this scenario, the trade secrets legal regime may provide effective quasi exclusive protection to the trade secret holder, particularly because the protection of factual exclusivity resembles the protection of possession under civil law traditions.[1974]

As a final note, it is worth highlighting that uncertainty remains as to how courts will interpret and apply the third prong of the trade secrets definition in the context of Big Data: the adoption of reasonable measures under the circumstances to protect the secret nature of the information.[1975] However, a survey of the most relevant case law in the U.S., England and Germany indicates that the threshold is rather low. In most cases, the adoption of legal measures (such as NDAs) and physical measures (such as the fragmentation of the information, building fences or encryption of the information) is deemed sufficient.[1976] After all, one of the primary justifications of trade secrets law is to avoid wasteful arms races in the adoption of measures to protect valuable undisclosed information. In this context, following the rationale outlined with regard to Cloud Disclosures, disclaimers of liability in the case of unauthorised access shall not prevent the application of trade secrets protection against third parties that access information unlawfully.[1977] In the same vein, the mere fact that Big Data sets are stored in the Cloud does not entail a disclosure of such information to the Cloud Service Provider, as long as there is no active transfer of knowledge between the parties.[1978]

1974 Herbert Zech 2016 n (278) 63-64; Michael Dorner 2013 (n 305) 111.
1975 Josef Drexl 2016 (n 426) 23.
1976 Chapter 4 § 3 E).
1977 Chapter 4 § 4 C) II. 6. b).
1978 Chapter 4 § 4 C) II. 6. b).

2. Additional problems: identifying the trade secret holder and the risk of infringement

As mentioned already, in the Data Economy, the traditional concept of value chains has been replaced by the value network one, and as a result the number of stakeholders involved in the production and analysis of data (of both a personal and industrial nature) has increased exponentially.[1979] Consequently, allocating the right over secret information is particularly complex. According to Article 2(2) of the TSD, the "trade secret holder" is defined as the individual or legal entity that has "lawful control" over the secret information. Yet, in the context of Big Data, there may be numerous stakeholders who are in control of secret information in a "lawful manner".[1980] Following the networked car example, (i) the company manufacturing the physical object in which sensors are included, (ii) the producers of the sensors, (iii) the owners of the car,[1981] or (iv) any of the licensees of the information can be regarded as trade secret holders under the definition provided in Article 2(2) TSD. This goes to show that in the Data Economy, the contours of the organisation and control between companies are progressively fading.[1982]

As a corollary to the foregoing, another salient issue that arises is the difficulty in the enforcement of trade secrets, as the entities engaging in the data analytics processes may infringe the alleged trade secrets if permission is not obtained from all of the stakeholders that are considered to be lawful holders of the information concerned under Article 2(2) TSD, by virtue of an assignment or a licensing agreement. Notwithstanding the aforementioned, following the rationale put forward above in the context of Big Data analysis,[1983] individual data will rarely qualify for protection. Only those persons or legal entities lawfully in control of large data sets, the specific arrangement of which remains unknown to other market participants in the form of combination secrets, will be entitled to claim trade secrets protection. Consequently, when a legal entity intends to carry out a data analytics process, it will only have to clear the rights with the holders of the data sets that contain the aggregated data, provided that compliance with

1979 Chapter 4 § 4 F) I.
1980 Herbert Zech 2016 (n 278) 64.
1981 Andreas Wiebe 2016 (n 287) 883 noting that there may no longer be trivial information.
1982 Andreas Wiebe 2016 (n 287) 883.
1983 Chapter 4 § 4 F) II.1).

data protection laws is ensured. Consequently, the number of stakeholders from which an assignment or license will have to be acquired is substantially reduced.[1984]

3. Conclusion on the applicability of the trade secrets liability regime to Big Data

Legal academia is divided on the potential applicability of the TSD to the protection of Big Data sets. On the one hand, Zech considers that the lack of transparency that governs the protection of IT matters calls for careful application of the TSD.[1985] In the same vein, Wiebe highlights that with time, it will become increasingly difficult to protect data as trade secrets, and consequently, the application of the TSD will be of little practical relevance.[1986]

Notwithstanding the aforementioned, the better view it is submitted, is the one purported by Dorner and Drexl. The former suggests that the trade secrets legal regime is applicable to Big Data analysis, as the protection of individual data is alien to IPRs and data input and output can in fact meet the requirements of protection laid down in the UWG, which regulates the protection of trade secrets in Germany.[1987] Similarly, Drexl is of the opinion that the tortious nature of the protection laid down in the TSD, centred upon the lawfulness of the means used to acquire, use and disclose secret information provides the most adequate legal framework to balance the interests of stakeholders in protecting their industrial data and the interests of third parties in accessing such data. Yet, he also mentions that "clarification of the scope of trade secret protection regarding data" would be welcome.[1988]

In this context, it is submitted that courts should follow the analytical framework suggested in the context of combination secrets to assess the eligibility of Big Data sets under the legal framework created by the TSD. This would ensure a balanced solution when delineating a company's private sphere vis-à-vis the public domain. In addition, it is also line with the

1984 This approach does not take into account the potential data protection issues that may arise.
1985 Herbert Zech 2016 (n 278) 64.
1986 Andreas Wiebe 2016 (n 287) 883.
1987 Michael Dorner 2014 (n 1960) 623.
1988 Josef Drexl 2016 (n 426) 66.

view expressed by most of the data holders that took part in the consultation launched by the Commission with regard to the "Building a European Economy Initiative", where it was noted that the Database Directive and the TSD provided sufficient protection to the investments carried out in data collection.[1989]

§ 5 Conclusion

A comparison of the definitions of a trade secret followed under the German and English jurisdictions before the implementation of the TSD reveals that despite substantial differences, both legal systems afford effective protection to valuable undisclosed information, as conceptualised under Article 2(1) TSD and in line with the minimum obligations established in Article 39(2) TRIPs. Notwithstanding this, in order to ensure uniformity across the 28 EU Member States, it is submitted that national courts should emphasise the need to establish causality between the value of information and its undisclosed nature. The concept of commercial value should be understood to refer to the ability to compete of the trade secret holder, which should be construed as including not only businesses, but also universities and research institutions. In addition, this thesis supports that the adoption of reasonable measures under the circumstances, which is not, as such, included as a normative standard in either of the studied jurisdictions, should be interpreted in a flexible manner in order to avoid wasteful arms races and promote the flow of information among market participants.

As regards the secrecy requirement, a review of the case law from the U.S., England and Germany has demonstrated that is not possible to extract a normative standard that is applicable in all circumstances to delineate the contours of protectable information and information that is in fact in the public domain. Ultimately, the assessment will depend on a number of factors such as whether substantial labour and intellectual skill are necessary to devise the secret and whether the trade secret holder retains control over the subsequent use and disclosure of said information. Consequently, it is submitted that the relative nature of secrecy is best as-

1989 Commission, 'Synopsis Report on the Consultation on the Building a European Data Economy Initiative.' (2018) 5 <https://ec.europa.eu/digital-single-market/en/news/synopsis-report-public-consultation-building-european-data-economy> accessed 15 September 2018.

sessed by reference to its boundaries with the public domain on a case-by-case basis. This is of utmost importance in order to determine the effect of disclosures in the digital age, which may be potentially automatically secrecy destroying. In this context, it is submitted that Internet disclosures and disclosures in the Cloud should be examined following the two analylitcal frameworks proposed, which place special emphasis on the actual access and the acquisition of active knowledge by the relevant circles. This thesis has also argued in favour of the protection of Big Data sets through trade secrets liability rules and in particular, through the application of the analytical framework proposed for combination secrets. By applying such a model, it is ensured that information in the public domain is not privatised therefore ensuring the equilibrium between the interests of the holders of secret information and the general interest in constructing a solid public domain.

In the light of the economic goals that the EU legislature ultimately intended to achieve with the adoption of the TSD, the following chapter focuses on the study of the strategic importance of trade secrets for certain industries and their increasing vulnerability through the application of the methodology of qualitative empirical research. To this end, the perfume industry is used as a study case to analyse the interplay between IPRs and trade secrets and the role that the latter play in appropriating returns from innovation in this manufacturing sector.