Conclusion

The so-called "Digital Revolution" has allowed companies and individuals to generate and share information faster than ever before. This has entailed radical shift in the traditional paradigm of creating, accessing, and transmitting information. Indeed, information has become a good few would still associate with scarcity and a lack of conveyance. Hence, it is no coincidence that in 2016 two major jurisdictions on both sides of the Atlantic sought to harmonise and strength the law of trade secrets. In May of 2016, the U.S. Congress passed the DTSA, while a month later, the Council adopted the TSD, following the approval by the EU Parliament. Such a legislative convergence evidences the strategic role that valuable confidential information plays for the competitiveness and growth of companies. However, as underscored throughout this dissertation, if trade secret legislation affords excessively wide protection, free speech and follow-on innovation might be set back. In light of the harmonisation goals pursued by the EU legislature, the primary aim of this study has been to examine the circumstances under which information loses its secret nature, with a view of finding a balanced solution to the optimal scope of secrecy.

The point of departure in such an appraisal is to understand the extent to which valuable information merits protection for the mere fact of being kept secret. As outlined in chapter 1, protection is justified both from a deontological and utilitarian perspective. However, utilitarian arguments appear to provide more solid grounds. To be sure, the law of trade secrets generates incentives to create information, even if not necessarily innovative. According to Duffy and Merges, it spurs market experimentation that allows undertakings to generate data. It also fosters cooperation and the sharing of information among market participants, even if such information is not ultimately disclosed to the general public. Furthermore, it allows companies to strike the optimal balance between the measures adopted to protect their secret information. Most importantly, it provides a Laboratory Zone in which companies can develop their innovations and market strategies without the interference of competitors. This is essential to ensure that patentable inventions are deemed novel and therefore eligible

for protection. As noted by the Commission, "every IPR starts with a secret".[2696]

Ultimately, such a statement begs the question of whether trade secrets should be considered as a form of property (or intellectual property) or instead as falling under the realm of unfair competition. In fact, a certain overlap may occur between the subject matter protected under the law of trade secrets and the patentable subject matter (and to a lesser extent copyright and the sui generis database right). Numerous studies show that when patents and trade secrets are mutually exclusive to each other, secrecy is the preferred method to appropriate returns from innovation. In this particular scenario, resorting to trade secret protection may undermine the disclosure function on which the patent system is built and may lead to a wasteful duplication of efforts, impairing competitive processes and follow-on innovation.

The dissertation has looked into the consequences of characterising trade secrets as a pure IPR or rather as falling under the realm of unfair competition rules and the implications that this may have on the scope of secrecy. Against this background, it has been submitted that the legal system for the protection of trade secrets presents an inherent hybrid legal nature. The relevant liability rules resemble unfair competition norms, whereas their enforcement seems very close to formal IPRs. Hence, in chapter 1 it has been argued that no legal consequences should derive from considering trade secrets as a form of intellectual property or as the object of unfair competition rules, i.e. the scope of protection should not be enhanced if trade secrets are regarded as IPRs. This is also the approach followed by the EU legislator in the TSD. Recital 16 merely sets out that the provisions of the Directive should not create any exclusive right on the information protected as a trade secret. Therefore, it seems that Member States are free to adopt either approach, as long as no absolute proprietary erga omnes rights are conferred upon the holder. The lawfulness of the conduct should remain at the centre of the assessment.

At the international level, Article 39 TRIPs laid down the minimum standards of protection, which created common ground across the EU jurisdictions, even though substantial differences in their implementation and the scope of protection persisted. Indeed, the requirements for protec-

2696 Commission 'Explanatory Memorandum, Proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure' 2.

tion set out in Article 39(2) have been included as the normative definition in Article 2(1) TSD. Hence, to merit protection information must be (i) secret; (ii) derive economic value from its secret nature and (iii) the holder must adopt reasonable measures under the circumstances to keep it secret. These are closely interconnected and ultimately reveal that the law of trade secrecy is concerned with the protection of the investment made in creating valuable information, but only against specific conducts that do not comply with the accepted market practices. Information is protected by the mere fact of being kept secret and providing its holder a competitive advantage. No additional qualitative threshold beyond secrecy has to be met. As a result, if the information is disclosed, the competitive advantage disappears. However, only if the acquisition, use or disclosure is carried out in a manner contrary to honest commercial practices, the holder of the information concerned will be able to seek legal redress.

The comparative analysis conducted in chapter 3 has underscored that despite the existence of common ground, prior to the implementation of the Directive, there were substantial differences in the regulation of trade secret protection across the Single Market and consequently, the level of protection varied substantially from one Member State to the other. For instance, regarding the liability of third parties, under German law conditional intent was required, whereas in England the threshold was much lower and referred to the observance of the standard of care followed by a honest person placed under the same circumstances. In addition, in Germany, it was unclear what remedies courts may award. Similarly, the assessment of the information that departing employees were free to use in their new positions and under which circumstances reverse engineering should be deemed lawful remained unsettled in both jurisdictions.

Against this background, in order to ensure the good functioning of the Single Market and to create a level playing field for the holders of valuable confidential information, the European Parliament passed the TSD, which was adopted by the Council on 8 June 8 2016, and which should be implemented in all EU jurisdictions before 9 June 2018. The Directive has managed to find a reasonable equilibrium between the interests of trade secrets holders in keeping their information concealed and the interest of third parties in accessing such information. To this end, the Directive sets out of a number of flexible and open-ended clauses, by virtue of which the appraisal of the lawfulness of a conduct is carried out by reference to the general standard of honest commercial practices enshrined in Article 10bis PC. The establishment of independent discovery and reverse engineering as lawful forms of acquiring a trade secret is crucial to strike such a balance

and to preserve the complementarity between the patent system and the trade secrets regime. In this context, the EU legislator has further laid down an array of exceptions to the rights conferred by a trade secret that safeguard the fundamental freedoms of expression and information and deem whistle-blowing lawful. Wisely, the applicability of these exceptions will ultimately depend on the balance of interests conducted by the competent national authorities. As a whole, the flexibility principle that informs the Directive, together with the minimum standards of protection, allows for considering all the relevant interests in each individual case and for adapting to future technological developments. However, it may result in divergent interpretations among Member States, thus hindering the ultimate harmonisation goals pursued by the EU lawmaker.

With regard to the secrecy standard, the TSD provides little interpretative guidance as to when information should be regarded as secret or as part of the public domain. This is mostly because the assessment of secrecy is of a factual nature and should be carried out on case-by-case basis. It is not possible to extract a normative test from the secrecy prong, unlike the novelty or inventive step requirements in patent law. Notwithstanding this, construing and defining the contours of private rights and the intangible objects to which they refer is of utmost importance in every legal regime.

Drawing on the foregoing conclusion, the dissertation has delved into the notion of secrecy by application of the methodology of comparative law, which has revealed that this standard is of a relative nature. Consequently, it is possible to share the information with a limited number of recipients, as long as the holder retains control and can prevent unwanted disclosures to third parties. According to Article 2(1)(a) if information is readily or accessible, it is automatically deemed part of the public domain. Ultimately, such an analysis is of an economic nature. If third parties with an interest can gain knowledge of the information concerned without incurring in great labour, intellectual skill or cost, the information should be regarded as readily ascertainable and thus, as being automatically part of the public domain. Conversely, secrecy is preserved if the interested third parties cannot acquire the information without that substantial amount of resources (i.e. undergoing the same intellectual development process as the trade secret holder). To hold otherwise would equate the secrecy standard to the absolute novelty standard followed in patent law and would render the secrets embodied in a product automatically part of the public domain upon their first sale. Instead, secrecy remains with regard to the intrinsic features or processes that can only be devised after the investment of sub-

stantial time, effort and cost. In particular, following the English case law, it has been submitted that the need to invest intellectual skill should be considered as the decisive factor that indicates that the information is secret. Ultimately, this is consistent with the utilitarian rationales analysed in chapter 1, by virtue of which, the law of trade secrets attempts to preserve the investment made in the creation of information.

The research has further attempted to conceptualise the notion of secrecy by reference to its negative dimension, i.e. when information enters the public domain. Taking a case-oriented approach, the effects of specific disclosures have been examined following the methodology of comparative law and a number of guiding principles have been proposed to ensure a homogeneous interpretation across the EU once the Directive is implemented. In view of the increasing vulnerability of information in the last decade, particular emphasis has been placed on the effects of disclosure in the digital age, such as disclosures to the state and its authorities, Internet disclosures, the protectability of combination secrets and cloud computing. In all of these instances, a dedicated analytical framework has been proposed to assess whether the information merits protection under the trade secrets liability regime. In this context, the suitability of resorting to trade secrets protection for Big Data sets has also been examined and an analytical framework to assess whether large streams of raw data may be legible for protection under the TSD has been suggested in order to avoid privatising information in the public domain.

In chapter 5 the perfume industry has been used as a study case to illustrate the increasing challenges that the holders of valuable information face in keeping it undisclosed. From a legal perspective the investigation has revealed that there is no single IPR that affords protection to perfumes as such. In addition, the empirical research conducted highlights that trade secrets play a central role in allowing scent manufacturers to appropriate returns from their creations an small incremental innovations. However, it has also revealed that their formulas can be reverse engineered at a very low cost by competitors, which reduces the incentives to create such products

The empirical analysis has further shown that secrets are most frequently ascribed to companies, which usually adopt physical and legal measures to protect them. In particular, in the adoption of these measures two distinct spheres can be identified. First, the internal sphere of secrecy, which refers to the preservation of confidential information within the company and mostly concerns employees, because they are the ones that regularly have access to valuable secret information in the performance of their duties.

Secondly, the external sphere of secrecy refers to the adoption of legal and physical measures in order to avoid the unauthorised use and disclosure of trade secrets by third parties such as suppliers, service providers, licensees or R&D partners that may have accessed the information with authorisation, but for a specific purpose. More generally, it also intends to preserve trade secrets from the interference of third parties. Consequently, chapter 6 has examined the relevance of contractual provisions (legal measures) to ensure secrecy in the two spheres identified.

During the course of the employment relationship, employees are bound not to disclosed trade secrets on the basis of a duty of loyalty. However, the application of such a duty in post-contractual scenarios appears more complex, particularly considering that the TSD provides that employees should not be prevented from using the skills, knowledge and experienced gained in the normal course of their employment in their new position. Hence, resorting to NDAs and non-competes appears to be the best way to conceal trade secrets from competitors. However, these agreements may negatively affect the career development of employees and stifle follow-on innovation. Consequently, the admissibility of such contractual provision is subject to different requirements in different Member States, as it has not been harmonised across the EU by the TSD.

The external sphere of secrecy refers to the preservation of confidentiality against the unlawful use and disclosure of trade secrets by third parties that may have accessed the information with authorisation from the holder but only for a limited time, or in order to achieve a specific purpose. This is typically the case of licensing agreements, where the trade secret holder grants the licensee the right to use the secret information in exchange for the payment of an agreed fee. In effect, in order to exploit trade secrets, their holders are required to carefully balance a number of competing interests. On the one hand, they should attempt to share the information with as few people as possible in order to limit the risk of disclosure and the resulting loss of the competitive advantage conferred by its secrecy. Indeed, once the information has left the internal sphere of the company, it cannot be reintroduced due to the inherently irreversible nature of cognitive processes: what has been learnt cannot be unlearnt.[2697] On the other, to maximise the economic potential of trade secrets, their holder may have to share the information with a substantial number of parties, particularly in the absence of funding resources, manufacturing capabilities or technical knowledge that allow for the development of the final product. Conse-

2697 Stefan Maaßen and Tobias Wuttke 2011 (n 2404) Rdn 38-40.

quently, the contractual clauses that regulate the use and subsequent revelation of trade secrets are in licensing and R&D agreements should be carefully drafted.

After examining the internal and external spheres of secrecy and its limitations, this dissertation has considered the possibility that secret information might never be unveiled, as some secrets are after all impenetrable. Therefore, it has been submitted that under specific circumstances, trade secrets protection should be finite, following the rationale applied in the Nordhaus model to justify limits in patent duration. However, it does not seem sound to set a fixed term of duration, such as for formal IPRs. In view of the casuistic nature of trade secret protection, it is argued that after some time protection should cease, even if the object of protection remains concealed. This would be best articulated by means of an exception in an infringement claim. The alleged infringer could counterclaim that trade secrets protection should not be enforceable if the dead-weight loss prevails in the above mentioned welfare trade-off. The problem, however, is that the information necessary to conduct such an assessment is, if at all, only in the possession of the trade secret holder. Third parties hence cannot evaluate in a reliable manner the point in time when the investment devoted to the development of the secret has been recouped and ultimately, from a welfare perspective, when they should be free to use the information.

Notwithstanding this, the dissertation has highlighted the relevance of contractual agreements in maintaining secrecy intra companies (with employees), but also extra companies (with regards to suppliers, licensees or R&D partners). Consequently, the thesis has propose to modulate the finite duration of secrecy protection by introducing a general presumption in the context of business-to-business agreements, by virtue of which the duration of secrecy and non-use obligations is limited to four years after the termination of the contract, unless the parties expressly agree otherwise.