The Protection of Data in our Digital Age

Associate Professor Andrew Beale OBE

Director of IP Wales® & Member of the International Institute of Shipping & Trade Law

Sue Ratcliffe

Swansea University

Professor Andrew Tettenborn

Member of the International Institute of Shipping & Trade Law

Legal protection of data

If land was the primary raw material of the agricultural age and iron the original raw material for the industrial age then data, as information in digital form, is the fuel of the information age. Since its creation data usage and storage has grown exponentially and remains a modern-day phenomenon. On one estimation, at the turn of this Century only 25% of information was stored in digital form but in the present day that has increased to over 95%[1] with 90% of the world's digital data only having been generated in the last few years[2].

1 James Manyika, Michael Chui, Brad Brown, et al., "Big Data: The Next Frontier for Innovation, Competition, and Productivity," McKinsey Global Institute, May 2011, http://wwwmckinsey.com/insights/business_technology/big_datathe_next_frontier_for_innovation, cited in Alec Ross, The Industries of the future (Simon & Schuster 2016) 154.

2 "Big Data, for Better or Worse: 90% of World's Data Generated over Last Two years, "Science Daily, May 22, 2013,

Understanding, analysing and forecasting from copious amounts of data is the role of *Big Data*[3], which enables us to examine in both smaller detail and larger scale than ever before.

The relevance of legal protection is limited. Just as good locks do more than any number of theft or burglary laws, the first line of defence for any firm concerned to safeguard its data, and especially its trade secrets, is physical measures. Any sensible business must take steps to make it less likely that their data will be compromised by prying eyes, computer hackers, cyber-pirates and all the myriad of other hazards inherent in the knowledge economy. So too with straightforward measures by a business to prevent its workers and collaborators from abstracting its data – especially undetectably – for their own benefit, or for that of third party competitors who might be prepared to pay generously for it. Such matters as copy protection for important documents and proper logging of all access to keys, swipe-cards and sensitive areas on a firm's server are vital[4].

---

http://www.sciencedaily.com/releases/2013/05/130522085217.htm., cited in Alec Ross, The Industries of the future (Simon Schuster 2016) 154.

3 Also known as Big Data Analytics, Analytics or Deep Analytics. The term as used in this sense seems to have originated in the 1990s: see The Origins of 'Big Data': An Etymological Detective Story, by Steve Lohr, which appeared in the op-ed column of the New York Times for February 1, 2013.

4 This will become slightly more important if and when the EU Trade Secrets Directive referred to below becomes law in the UK: under the Directive, a trade secret eligible for protection must have "been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret" (Art.2(1)(c)).

What is also necessary, however, is a simple and straightforward background of legal protection when things go wrong and data is misused or ends up in the wrong hands. Simplicity and predictability are particularly important here. Start-ups and Small-Medium Enterprises (SMEs) tend to have relatively low capital bases, and a correspondingly large proportion of their exploitable assets tied up in manufacturing or commercial secrets and similar intangibles. They are just the firms who cannot afford to divert large sums to legal advice and litigation over obscure legal provisions relating to the protection of these assets.

Since 1995 a minimum legal standard of protection for intellectual property has been prescribed for all member States of the World Trade Organization[5] under the TRIPS agreement[6] . Under Article 39, what is referred to as "undisclosed information"[7] is recognised as an undefined category of 'intellectual property", protectable not on the basis of its content, be it in digital form or otherwise, but by reason of its commercial worth and "undisclosed" nature. Based on the provisions of U.S. Uniform Trade Secrets Act of 1985[8]

5 A category covering virtually all the world's major trading states, including all of Europe (apart from the Vatican).

6 More precisely, the 1994 Agreement on Trade-Related Aspects of Intellectual Property Rights. Its aim is to provide for minimum levels of cross-border protection for intellectual property rights within the context of the WTO trade regime.

7 Often also called "trade secrets" or "know-how".

8 Uniform Acts in the US context have no legal force of their own. They are merely texts produced by a semi-private body of lawyers and professors, the Uniform Law Commission (established in 1892), for possible State adoption in State legislation. The text of the 1985 Uniform Act, which updates a previous draft of 1979 and has been widely adopted by State legislatures, is available online at

the Article sets as the conditions for protection: it must be secret, possess a commercial value, be the subject of reasonable steps (in the circumstances) to remain secret. Whilst the Article's negotiation led to legal debate about whether trade secrets could be considered "property" under law, the issue was deftly avoided by adopting the European proposal to link the protection with unfair competition under Article 10bis of the Paris Convention,[9] already adopted into TRIPS under Article 2. It remains, however, that there can only be "possession" or *de facto* "control" of data as "undisclosed information" as opposed to legal "ownership"[10]. Further protection is also afforded under the Article to "undisclosed test or other data" for the pharmaceutical and agrochemical industries, provided the origination of the data has involved "considerable effort"[11]. Only a few countries had developed legal rules to protect test data before the TRIPS negotiations, so again heavy reliance was placed on the U.S. position and its recognition of data exclusivity[12]. The Article is accordingly protective of test data where its submission is required for marketing authorization, is not publicly available and refers to a "new chemical entity".

---

http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf [consulted 7 December 2016].

9 That is, the 1883 Paris Convention for the Protection of Industrial Property, as subsequently amended.

10 J.H.Reichman, Universal minimum standards of intellectual property protection under the TRIPS component of the WTO Agreement, The International Lawyer 1995, vol. 29, No. 2, p.378, cited in UNCTAD-ICTSD, Resource Book on TRIPS and Development (Cambridge University Press 2005) 521.

11 Article 39.3.

12 See Zhiwen, L. 2014. TRIPS – Plus Protection on Drug Innovation under US FTAs. Journal of Comparative Law, 1, p.010.

In addition to being the first international convention to impose specific legal protection on undisclosed information, including test data, TRIPS also requires protection for the "compilations of data or other material, whether in machine readable or other form…Such protection, which shall not extend to the data or material itself, shall be without prejudice to any copyright subsisting in the data or material itself"[13]. But whereas the Berne Convention[14] requires originality in the selection "and" arrangement of collections for copyright protection, TRIPS only requires originality in the selection "or" arrangement for database protection as an intellectual creation, irrespective of whether copyright already protects individual parts of that creation or not[15]. It should be noted however that "copyright protection for compilations of data has different economic and social implications to the *sui generis* right currently in place in the European Union…designed to protect a particular kind of investment (i.e. primarily economic) with a view to encouraging optimal levels of production of databases"[16].

How is data defined?

13 Article 10.2.

14 The Berne Convention for the Protection of Literary and Artistic Works of 1886, as subsequently amended. This Convention is the bedrock of most international copyright protection.

15 UNCTAD-ICTSD, Resource Book on TRIPS and Development (Cambridge University Press 2005) 164.

16 UNCTAD-ICTSD, Resource Book on TRIPS and Development (Cambridge University Press 2005) 170.

So how is “data’ defined under the laws of England and Wales? The Oxford English Dictionary defines “data” as an item, or collection of items, of information.[17] The definition of data as being “information” also neatly corresponds to its treatment in the Data Protection Act 1998, where data is defined as information which inter alia includes information that:

(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,

(b) is recorded with the intention that it should be processed by means of such equipment,

(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system.

This definition, even though the 1998 Act is not directly relevant to commercial information,[18] is nevertheless helpful and informative. It is clear from it that data which is in existence is covered by headings (b) and (c), since it is or has been recorded with a view to it being processed. However, if we look at heading (a) the definition of data also covers information that is undergoing processing. Processing information is done by computer equipment using algorithms to extract content and useful material from existing information/data and incorporate it into some form of use to the party processing it, such as a filing system or CAD application. Therefore, processed data is just as much to be classified as “data” as raw information is. The pre-existing data could exist on one set of servers then be processed

17 The relevant parts of the definition are as follows: “1. As a count noun: an item of information; a datum; a set of data …. 2. As a mass noun. a. Related items of (chiefly numerical) information considered collectively, typically obtained by scientific work and used for reference, analysis, or calculation …”.

18 Its aim being essentially to protect personal data on individuals from misuse or unjustified disclosure.

and communicated to, say, a server belonging to a third party, such as Amazon, or a “cloud” provider, who hold data for its customers. The data that could be collected is vast ranging from customer information and transactional histories to experimental results and clinical research data. Particularly useful data is collected through cookies on web sites as to buying patterns of individuals, web-sites visited and products reviewed and this data can then be processed to form new data which can all be used for target marketing. Clinical data, which again is often based on patient data that has been processed, for example by anonymizing, and this processed data is particularly valuable in that it is used to support the Regulatory approval of new drugs. Therefore it is clear that data as defined by the Data Protection Act covers information that has considerable value. However, the Data Protection Act relates to personal information relating to an individual rather than data *per se* which could be company information that not necessarily relates to an individual, for example anonymised patient data.

The available legal protection

How well, then, is data legally protected in England and Wales? In theory, the answer is that civil law protection is good: so much so that in 2014 the House of Commons' European Scrutiny Committee claimed that, apart from a technical point on limitation law, our law already conformed with the then draft of what is now the EU Trade Secrets Directive[19].

19 Formally, Directive (EU) 2016/943 of the European Commission on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, was adopted by the European Parliament and the Council on the 8th June 2016 as requires EU countries to bring into force the requisite

In summary, the scheme is as follows.

First, in common with most other legal systems, English law unequivocally imposes on anyone directly entrusted with confidential data, whether worker [20] or independent contractor[21], an implicit duty owed to the entruster in contract not to misuse it[22]. Anyone guilty of breaking that duty is liable in damages for all the foreseeable consequences of that breach[23], and can equally be prevented by injunction from misusing it[24]. Anyone knowingly suborning another to break this contractual duty, or receiving information from someone who they know is breaking it by revealing the information, is liable in tort for inducing breach of contract[25]. Furthermore, so long as such data remains confidential and cannot be regarded as having entered the public domain, anyone in possession of it who knows its origin can

---

laws and administrative provisions by 9th June 2018. Following a change in the draft, the limitation point has since fallen by the wayside.

20 Stemming from the early decisions in Lamb v Evans [1893] 1 QB 218 and Robb v Green [1895] 2 Q.B. 315; F.Gurry, Breach of Confidence (2nd ed), Chap. 12.

21 See the early case of Mechanical & General Inventions Co Ltd v Austin [1935] A.C. 346; F.Gurry, Breach of Confidence (2nd ed), Chap. 13.

22 See generally F.Gurry, Breach of Confidence (2nd ed), Chap. 4.

23 F.Gurry, Breach of Confidence (2nd ed), Chap. 19.

24 F.Gurry, Breach of Confidence (2nd ed), Chap. 18.

25 F.Gurry, Breach of Confidence (2nd ed), paras.2.120 ff.

equally be prevented in equity from using it and may be liable in compensation if he does so[26].

Secondly, subject to the limits on contractual freedom imposed by the doctrine of restraint of trade[27], express contractual protection can also effectively restrict the uses to which data can be put. Hence where an airline puts details of its flights on its website, it can legitimately prevent "screen-scraping" by other merchandisers and aggregators for their own purposes[28], even where no other independent intellectual property is available and thus the information would otherwise be subject to a free-for-all[29].

Thirdly, the English law of tort is strong – perhaps one of the strongest in the world – on the protection of tangible property. This can be surprisingly important for the protection of data generally. Most obviously, the law of trespass covers all physical incursions on property,

26 For the development of this jurisdiction, see Breach of Confidence (2nd ed), paras.2.005 ff.

27 See Chitty on Contracts (32nd ed), paras.16-085 ff.

28 For an instance of a claim of this sort, see the Irish decision in Ryanair Ltd v Bravofly Ltd [2016] IESC 53 (a case still in the preliminary stage). Note that restrictions of this sort are permissible under EU intellectual property law, even where data is otherwise outside IP protection: see the decision of the ECJ in Ryanair Ltd v PR Aviation BV [2015] 2 C.M.L.R. 36.

29 This is permissible under EU intellectual property law because of the decision of the ECJ in Ryanair Ltd v PR Aviation BV [2015] 2 C.M.L.R. 36.

whether real[30] or personal[31]. It follows that where a defendant enters a part of premises where he is not permitted to be, or physically accesses some tangible medium containing data, any losses suffered as a result are compensable[32], including presumably those stemming from the loss or taking of the intangible data there[33]. Indeed, it may well be that liability goes even further than this and extends to any unauthorised access, whether directly or via cyberspace, to a computer in a claimant's possession[34]. If this is right, it provides a cast-iron legal means of redress in respect of most pilfering of data, whether secret or not (for example, information aggregated on computer storage where it is clear that no consent is given to its wholesale use by a competitor)[35].

30 Where the cause of action is trespass to land: Clerk & Lindsell on Torts (21st ed), Chap. 19.

31 In the case of trespass to goods: Clerk & Lindsell on Torts (21st ed), Paras.17-131 ff.

32 Pritchard v Long (1842) 9 M & W 666 (semble). A more colourful example is Bracegirdle v Orford (1813) 2 M & S 77.

33 Compare the decision in White v Withers LLP [2009] EWCA Civ 1122; [2010] 1 F.L.R. 859 (not on commercial information but still in point).

34 For the authorities, see Clerk & Lindsell on Torts (21st ed), Paras.17-135-136. The limitation to a machine or server in the claimant's possession is important. In so far as data is kept in the 'cloud', then it is suggested that the only liability in trespass is to the owner of the server unless access was gained physically via the victim's own machine.

35 Compare the American decisions in eBay Inc v Bidder’s Edge Inc, 100 F.Supp.2d 1058 (N.D. Cal. 2000) and Snap-On Business Solutions Inc v O'Neil & Associates Inc, 708 F.Supp.2d 669 (2010).

Fourthly, it is now clear that English law protects against the wrongful alienation of transferable rights, including it seems intellectual property rights. It has to be remembered that ownership of such rights may be transferred in fraud of the owner. For example, a senior rogue employee or consultant armed with ostensible authority to deal with the Intellectual Property Office might quite easily cause the rights to a complex registered design right to be transferred to a series of third parties[36]. As regards anyone knowingly responsible for such a transfer and in addition any recipient who knows or has good reason to know of the irregularity, the owner has a claim for damages[37].

Apart from the above, we can of course add “front-line”, overtly IP-based, protections. Two of these are essentially EU-based (and therefore, unless and until Brexit becomes a reality, beyond UK or Welsh government control). One, surprisingly important in practice, is the already referenced database right[38], partly overlapping with copyright (in cases where there

36 A simple enough process: the transfer form, Design Form DF12A, is a mere page-and-a half long and takes about two minutes to complete, with (it seems) only a limited check on authenticity. Theoretically the same thing could happen with copyright, though it is less likely.

37 Armstrong DLW GmbH v Winnington Networks Ltd [2012] EWHC 10 (Ch); [2013] Ch. 156 (actually about another form of intangible rights, but the reasoning equally would apply to intellectual property rights).

38 See the Copyright, Designs and Patents Act 1988, ss.3A, 50D, 296B, embodying in the law of England and Wales Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases.

is an evident high degree of human ingenuity and originality)[39], but going a good deal beyond it, so as to protect from copying and publication[40] any collection of information[41] involving a substantial investment of effort in research or data gathering[42]. Admittedly the protection this gives may be limited; for example it would not, it seems, cover computerised stores of raw scientific research data, nor yet basic production figures or details of manning levels or profit forecasts[43]. Nevertheless, once a degree of processing of the data has intervened, then protection automatically kicks in. Thus, it is suggested that the Database Directive[44] is likely

39 Note that this is a more exacting requirement than the requirement for copyright generally in common law countries, where not a great deal of intellectual input is required for copyright to subsist: a point well made in the December 2005 DG Internal Market and Services Working Paper (First evaluation of Directive 96/9/EC on the legal protection of databases), paras.1-2.

40 Database Directive, Art.7.1.

41 Whether electronic or not: see Database Directive, Art.1.2 (“collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means”).

42 See Database Directive, Art.7 (requirement for “qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents”).

43 Because of the CJEU's decision in British Horseracing Board Ltd v William Hill Organization Ltd (Case C-203/02) [2005] 1 C.M.L.R. 15, excluding data not gathered, but actually produced, by the database holder (there the names of horses entered for races).

44 It is often the case that value in data lies in the way it is formulated into a database and its ease of extraction from that database. This is certainly the case if the data is from

to provide a potentially useful level of protection in respect of such “added-value” business tools as production analyses, financial spreadsheets and itemised customer lists[45]. Again, for those businesses involved in the development of computer hardware, another

public record sources that are available for anyone to extract that piece of data. However, where information is extracted and processed to form data as defined in the Data Protection Act then there is arguably value in this data as added value has been given to the data by processing it. The processed data may be information about an individual and their buying habits which could have considerable value for a marketing company. Although a database of such information is valuable there is also value in the individual data. If this information can be connected to an individual its use is curtailed via the Data Protection Act but should the data become anonymised or not relate to an individual per se then there is little protection for anyone creating the data beyond the use of trade secrets. It is clear from case law such as William Hill (see footnote above) that individual data is treated very differently from the database. Also, if there is not a high enough level or originality to attract copyright protection again there is no protection for the data itself unless it can be viewed as being a substantial part of the database. Although the EU had the intention of harmonising laws under the Directive, infringement issues are decided according to national law, so if data is being transmitted overseas or uploaded onto external servers the effect of database rights under the Directive may be limited.

45 See British Sky Broadcasting Group Plc v Digital Satellite Warranty Cover Ltd (In Liquidation) [2011] EWHC 2662 (Ch); [2012] F.S.R. 14 and Flogas Britain Ltd v Calor Gas Ltd [2013] EWHC 3060 (Ch); [2014] F.S.R. 34.

specialised example is a limited protection accorded to certain kinds of computer chip design[46].

The database right aside, in practice the law of copyright is also extremely important as a protector of data. This is for several reasons. One is that, while it is possible to abstract or misuse data by reading, memorising and utilising it, the vast majority of data misuse in practice involves copying, whether cut-and-paste on a screen or scanning a piece of paper. The second is that a major subject of data breach, computer software, is by universal consent (and EU law[47]) the subject of copyright[48]. Thirdly, despite the adage that there is no copyright in ideas but only in their expression, English and Welsh copyright in practice protects almost any written document, including a document on a computer disk drive, of any length. In contrast to the situation with (say) German law[49], which explicitly requires a

46 Which applies a modified version of Part III of the Copyright, Designs and Patents Act 1988 to such items: see the Design Right (Semiconductor Topographies) Regulations, SI 1989/1100 and the Amendment Regulations of 2006, SI 2006/1833. The source is Euro-law: see Council Directive 87/54/EC.

47 See the Software Directive 2009 (Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs).

48 Generally W.Cornish, D.Lewellyn & T.Aplin, Intellectual Property (8th ed) Chap.20.

49 It is worthy of note that Chinese IP laws from the mid 1980s were modelled on the German Civil Law IP system.

degree of personal creativity[50], the requirement for originality or intellectual input is minimal[51]. And lastly, as before there is no difficulty in holding a copyright infringer liable for damages for any consequential losses resulting from the breach[52]. No wonder, then, that many commercial claims for abstraction of information or data are framed as claims for breach of copyright as well as for breach of confidence.

So far so good. What is less satisfactory as regards the law of England and Wales is the issue of certainty and accessibility. In some cases the problem is technical. For example, the nature of the remedy for breach of confidence – not technically a claim for damages but for equitable compensation – creates a peculiarity on the European level as regards jurisdiction against defendants domiciled elsewhere in the EU[53]. More to the point, however, is the law's lack of accessibility to even a reasonably well-educated layperson or business owner. True, classic rights such as copyright are now codified, albeit in the Copyright, Designs and Patents Act 1988, a statute of great complexity, and some answers are

50 See Urheberrechtsgesetz, §2.2 (protected works stated to be nur persönliche geistige Schöpfungen); generally, E.Rosati, “Towards an EU-wide copyright? (Judicial) pride and (legislative) prejudice” [2013] I.P.Q. 47.

51 W.Cornish, D.Lewellyn & T.Aplin, Intellectual Property (8th ed) Para.11-08.

52 H.Laddie, P.Prescott & M.Vitoria, The Modern Law of Copyright, Para.39.40.

53 Put briefly, a trade secret owner can always sue here for an infringement in England if it amounts to a breach of contract or tort: Brussels I, Art.5. But if he has to sue for breach of confidence and the defendant is domiciled elsewhere in the EU he has to sue there under the residual Art.4. See Kitechnology BV v Unicor GmbH Plastmaschinen [1994] I.L.Pr. 568; [1995] F.S.R. 765; Vidal-Hall v Google Inc [2015] EWCA Civ 311; [2015] 3 W.L.R. 409 at [46].

available after a fashion to anyone prepared to plough through it and the parallel EU legislation. But elsewhere matters are less straightforward. Take, for example, the rules protecting trade secrets under contract law and breach of confidence. None of this is codified at all; to understand them the manager of a SME either has to have them summarised by his lawyer, or to plough through a welter of case-law or a practitioner's text-book. To take as one instance the contractual duty of an employee, what can be gleaned from the decided cases is that this consists, fairly vaguely, of an implied term against disloyalty. This may of course include copying or memorising trade secrets with a view to using them for one's own benefit or that of another, and in certain cases actually using them, but subject to the qualification that fair competition is allowed, including making preparations during employment for competitive activities to be undertaken after it. Again, the equitable doctrine of breach of confidence is not much more precise. There must, it seems, be a piece of information[54], or at least an idea or concept, with some degree of originality[55] and exactitude[56], and not in the public domain, in the sense of being relatively easily available to anyone who cares to look for it[57]. And there must have been disclosure in confidence, an

54 Which may of course exist in nature as much as in human expression: for instance, a cutting containing DNA (as in the Australian decision in Franklin v Giddins [1977] Qd.R. 72). A sample of a drink made according to a secret formula would be a good example.

55 And not something entirely banal or trivial: Deloitte & Touche LLP v Dickson [2005] EWHC 721 (Ch) at [38] (Laddie J).

56 A vague plan or imprecise concept will not do: eg De Maudsley v Palumbo [1996] E.M.L.R. 460 and Sales v Stromberg [2006] F.S.R. 7.

57 F.Gurry, Breach of Confidence (2nd ed), paras.5.14 ff; Douglas v Hello! Ltd (No.6) [2005] EWCA Civ 595; [2006] Q.B. 125 at [105] (Phillips MR).

obtaining by reprehensible means[58], or an incidental obtaining of obviously confidential material[59]. The position of third party recipients of secrets remains obscure. While they can probably be prevented from using information if they knew it was secret when they got it or if they received it gratuitously, there is no unequivocal indication what the position is if they have paid for it in all innocence[60]. The matter is further complicated by the existence of a number of overriding defences, such as reverse engineering and a general public interest defence.

Compare this with other jurisdictions. In Germany, for example, despite complaints from German lawyers about its untidiness, most of the law on trade secrets appears clearly and succinctly in three sections of the Unfair Competition Law, taking up about 500 words[61].

58 Such as theft (as in Franklin v Giddins [1977] Qd.R. 72), phone-tapping (Francome v Mirror Group Ltd [1984] 1 W.L.R. 892), or illicit photography in a private place contrary to a clearly enforced ban (as in Creation Records Ltd v News Group Newspapers Ltd [1997] E.M.L.R. 444 or OBG Ltd v Allan [2007] UKHL 21; [2008] 1 A.C. 1 (as regards Douglas v Hello! Ltd).

59 For example, a document marked “Private” blown out of a window (see Lord Goff in Spycatcher [1990] 1 A.C. 190, 281) or a clearly mistaken delivery (English & American Insurance Co Ltd v Herbert Smith [1988] F.S.R. 232).

60 F.Gurry, Breach of Confidence (2nd ed), Paras.7.122 ff; P.Stanley, The Law of Confidentiality: A Restatement, Chapter 19; D.Vaver, Reforming intellectual property law: an obvious and not-so-obvious agenda: the Stephen Stewart Lecture for 2008 2009 IPQ 143, 157.

61 UWG (Gesetz gegen den unlauteren Wettbewerb), §§ 17-19. This is admittedly not the only source of the law: the general contractual duty of good faith may also be invoked on

These ban, in simple terms, the misappropriation of secret data by employees, its dishonest abstraction, receipt or exploitation by third parties, its misuse by those entrusted with it, and the suborning of others to divulge it. Infringement is a crime and a tort[62]. Again, in the US too the matter is largely codified (although a few states still rely on common law protection, with all the disadvantages this entails). As regards state law, most states have adopted the Uniform Law Commission's Uniform Trade Secrets Act, dating from 1979 and updated in 1985[63]. This is a relatively short provision, running to six substantive sections[64], which having defined a trade secret widely[65] creates a general right to damages and injunctions in

---

occasion to protect secrets, and explicit non-disclosure agreements are common. Nevertheless, the UWG is a good start.

62 A tort because the Civil Code (BGB), §823.2, provides that criminal prohibitions aimed at protecting third party interests (Schutznormen) give rise to civil liability in so far as infringed deliberately or culpably.

63 Text available at http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf [consulted 7 December 2016]. For an example of a state enactment of it see Connecticut General Statutes, § 35-50 to 35-58. A few states have their own legislation: e.g. Massachusetts General Laws, Ch.93, §§ 42-42A (1993).

64 Technically it has 12 sections, but the final six deal with ancillary matters such as its relationship with other laws, the need for uniform construction, etc..

65 See s.1(4) ("information, including a formula, pattern, compilation, program, device, method, technique, or process, that (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or

respect of appropriation by unlawful or unfair means[66]. Parallel to this, at the federal level trade secrets related to products or services used in interstate or foreign commerce are protected by the Economic Espionage Act 1996 (as amended)[67]. This provision, again fairly short and straightforward, is mainly aimed at making abstraction of such trade secrets a crime[68], but incidentally also creates a right to injunction and damages[69].

Looking to the future

Will the matter be improved with the new Trade Secrets Directive [70], a minimum harmonisation proposal for the civil law? It has been suggested that English law already complies with the Directive anyway[71]; but this complacency might be misplaced, and at least some small changes may be required: for instance, an explicit requirement that to be protected the holder of a secret must be shown to have taken reasonable steps to protect it,

---

use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.").

66 See ss.3-4.

67 See 18 USC §§ 1831 et seq.

68 18 USC § 1832. § 1831 provides for increased penalties where the secret is abstracted for the benefit of a foreign organisation.

69 18 USC § 1836.

70 Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

71 See the Commons European Scrutiny Committee discussion of the Directive in its thirty-sixth report for 2013-2014, 12 February 2014 (HC 83-xxxiii, Chapter 3).

and a limitation on the compensation that can be awarded against an innocent infringer. More to the point, however, the Directive may well as a codifying measure improve matters as regards accessibility. For example, what counts as a “trade secret” is defined; the acts amounting to infringement are described in detail; it is made clear that a remedy is available even against good faith purchasers of a trade secret; defences such as disclosure in the public interest, and workers' rights to make use of acquired skills, are expressly provided for; minimum remedies are laid down; and so on. Admittedly there are some difficulties, in particular as regards remedies. The measure of damages, for example, is unclear. In principle this is based squarely on loss[72], which is appropriate in the context of commercial information. But the waters are then muddied. “Moral prejudice” is to be compensable[73], which seems odd in the context of a measure aimed at the protection of commercial information. Furthermore, there is a requirement to take account of “any unfair profits made by the infringer”[74], which seems to take the remedy away from compensation and closer to an account of profits. Furthermore, there is a provision that should worry any SME concerned for its cash-flow and financial planning. The power of a court to refuse an injunction against the use of a trade secret on the grounds of hardship (“disproportionate harm”) is preserved[75]: but there are two stings in the tail. First there is a strict requirement that at the time of use of the trade secret the defendant neither knew nor ought to have known of any prior wrongful dealings; and secondly it seems that a defendant seeking to avail itself of this exception must be prepared to pay a licence fee for the whole time during

72 See Art.14(1) (“… damages appropriate to the actual prejudice suffered as a result of the unlawful acquisition, use or disclosure of the trade secret. ...”).

73 Art.14(2).

74 Art.14(2).

75 Art.13(3).

which it has used the trade secret. In short, a defendant which has in all innocence invested substantial sums in establishing a line of business is likely to be faced with the unenviable choice between either writing it off or paying considerable back royalties for the entire period it has been using the secret in question. A more effective discouragement to innovation would be difficult to imagine.

Conclusion

In large measure the existing legal protection of trade secrets data is limited due to a low level of legal protection[76], issues of legal fragmentation both across and within differing ~~legal~~ jurisdictions around the world and problems associated with poor civil redress and criminal enforcement, including a failure to protect the confidentiality of trade secrets during legal proceedings. Difficulties in finding an agreed understanding of "trade secrets" and "know-how" resulted in TRIPS adopting the more neutral term "undisclosed information", whilst at the same time refusing to offer any legal definition as to its meaning. In consequence, a recent study by the World Trade Organization has found that legal protection of confidential information in its member states today derives from over 25 different fields of law[77].

76 Trade secrets are non-exclusive, so it is not a misappropriation to independently discover the secret information or otherwise reverse engineer it from a properly obtained source. Moreover, trade secrets have been described as "too slippery" for any higher legal protection because information is not treated in law as property - see Robin Jacob, Daniel Alexander QC & Matthew Fisher: Guide book to intellectual property (6th Edition Hart Publishing 2013) 205.

77 WIPO (2013) Survey on Technology Transfer Agreements and Antitrust. Geneva.

Moreover, TRIPS was negotiated at a time when the usage and storage of digital data was in its infancy, a global economy underpinned by employee mobility was still in creation and the notion of globally dispersed research and development (R&D) driven by what was to become known as "open innovation" remained ~~still to be~~ undiscovered by the boards of most large multi-national ~~corporation~~s. A Report[78] published by the World Intellectual Property Organization in 2015 would suggest that until the global community addresses the issue of legal fragmentation it will remain a largely unsatisfactory civil law environment for Start-ups and SMEs, which are heavily reliant on their trade secrets and know-how[79], to be expected to grow their businesses within the global economy. So does the protection of sensitive data fare any better under the criminal law?

Lord Boyle has noted sardonically, "it is not too much to say that we live in a country where…the theft of the board room table is punished far more severely than the theft of the board room secrets"[80]. This situation is in marked contrast to the US where the Economic

78 WIPO (2015) Private International Law Issues in Online Intellectual Property Infringement Disputes with Cross-Border Elements

79 QED Intellectual Property (2003) Evaluation and Validation of Intellectual Property by IP Wales Grant Award Candidates – commenting on the finding that respondent companies only identified 14% of their IP to be know-how & 7% trade secret the authors concluded, "we would have expected to see know-how showing a higher percentage than patents (35%), as SME's typically trade on their know-how and levels of expertise. This perhaps suggests that the respondents may undervalue their know-how (& trade secrets, given all patentable inventions essentially begin their life as trade secrets – see Pooley, 1997), possibly because it does not represent formal IP like a patent or trade mark.

80 Legislating the Criminal Code: Misuse of Trade Secrets consultation paper http://www.lawcom.gov.uk/wp-

Espionage Act 1996 (as amended) contains a separate provision to criminalise the commercial theft of trade secrets and preserve their confidential integrity during any criminal proceedings[81]. Nevertheless, the storing and processing of digital information on external servers, which allows trade secret theft to be initiated from anywhere in the world is a growing threat under IP cybercrime[82] and adds a third dimension to online IP crime, which has traditionally been viewed as just combating counterfeiting and piracy[83]. The growing threat of IP cybercrime led in 2013 to the UK Intellectual Property Office funding PIPCU [City of London Police Intellectual Property Crime Unit]. Whilst PIPCU has reported success in disrupting borderless online IP crime[84] it recognises that it cannot hope to eradicate it because equally mobile cybercriminals reside outside its territorial competence (and, as

content/uploads/2015/03/cp150_Legislating_the_Criminal_Code_Misuse_of_Trade_Secrets_Consultation.pdf (accessed 24/8/16).

81 See 18 USC §§ 1832 & 1835.

82 Jennifer Brant and Sebastian Lohse, Trade Secrets: Tools for Innovation and Collaboration [2014] International Chamber of Commerce (ICC) 5.

83 "Whereas online trade mark abuses (e.g. counterfeit goods) and copyright infringements (e.g. illegal downloads) are well documented our understanding of the relevance of the linkage between IP Crime & eCrime to the SME sector (e.g. the taking of confidential information) is still in its relative infancy" - Jane Foulser McFarlane, Legal Counsel for IP to the National Assembly for Wales (2009), Report Prepared for the Welsh Assembly Government on IP Crime & E Crime (IP Wales) 3.

84 Under Operation Creative an Infringing Website List (IWL) was created resulting by 2015 in a 73% drop in advertising commissioned on copyright infringing websites.

often as not, outside the EU)[85]. So for the present, at least, tangible measures remain the primary effective mechanism for the protection of data in our digital age for the majority of Start-ups and SMEs.

The growing fondness for storing and processing sensitive data in the 'cloud' raises important issues of cybersecurity and inappropriate access by third parties. However, recent research commissioned by Trend Micro would suggest that the vast majority of ~~S~~start-ups and SMEs are currently operating in ignorance of the threat posed[86]. This research finding resonates with earlier research commissioned from IP Wales by the Welsh Government which concluded that "the lack of awareness of security risks… is astonishing in a digital age, which boasts a high level of sophisticated IT crime"[87]. The threat currently confronting

85 See Rob Mackinlay, 'Disrupting borderless online IP crime' (CILIP Update March 2016) 39.

86 Vital Statistics on behalf of Trend Micro (August 2015) – "In the United Kingdom, as in many other economies around the world, smaller businesses are the lifeblood of national prosperity. In essence SMEs 'are' the private sector, according to the Department for Business, Innovation & Skills, they employ more people (60% in the UK in 2014) and generate almost half the total turnover of the private sector (48% in the UK in 2014)…We interviewed 500 key decision makers and business owners in UK SMEs to compile the research. Amazingly, only half of them said they rely on internet security tools…Three-quarters (74%) admitted to not fully understanding the legal implications of a cyberattack…Tellingly just 18% said they thought their data was worth stealing".

87 Jane Foulser McFarlane, Legal Counsel for IP to the National Assembly for Wales (2011), Intellectual Property Rights Infringement and Enforcement Issues in IP Wales Funded Businesses (IP Wales) Conclusion para. 7.

Start-ups and SMEs largely consists of three main types of cyberattack one of which, Network Confidentiality, specifically targets trade secret data.

We have already ~~referenced~~pointed out ~~-~~the familiar value of a secure lock to protect the tangible property of a business, this being ~~and this is~~ often supplemented by a burglar alarm. But, ~~but~~ unlike the burglar alarm which can only alert~~s~~ the business to an intrusion and possibly scare the intruders off~~hopefully deters~~, cybersecurity can proactively protect the intellectual assets of a business by blocking the majority of intrusions into the network before they happen~~infection~~. It can rapidly detect and remediate any infection which has already infiltrated the network. It can also stop data breaches from lost or stolen end points (desktops, laptops, tablets, smartphones, USB sticks etc.); safeguard online financial transactions; secure password management; and manage back-ups. It can even pre-empt future data attacks via automated risk assessments.

As mission critical as passive cybersecurity protection measures may be for any IP-~~-~~active business with an online presence, few Start-ups or SMEs will find themselves in the financial position to be able to afford the type of expensive cybersecurity protection that governments and multi-national corporations can afford. In this respect Alec Ross, Senior Advisor for Innovation to Hillary Clinton as Secretary of State notes cybersecurity "is supposed to be a public good administered by government, not a private good purchased in the marketplace…Government has a responsibility to protect its people, not just its big business and infrastructure…but there is an as yet unmet obligation by government to define its responsibilities to its citizens in this newest domain of conflict"[88].

88 Alec Ross, The Industries of the Future, (Simon & Schuster, 2016) 151.

At the time of writing it remains to be seen whether the UK government post ~~B~~-rexit will continue to commit to inter-state co-operation on cybersecurity and the creation of an open, safe and secure cyberspace within Europe[89]. The creation in October 2016 of the UK's first National Cyber Security Centre (NCSC)[90], committed to help make the UK "the safest place to live and do business online"[91], broke new ground by additionally committing the UK to an "Active Cyber Defence" programme[92]. A Report published in the same month by the George Washington University Center for Cyber and Homeland Security (CCHS) noted that in terms of private sector active defence against cyberattack this now places the UK in comparison with the US, albeit with some "ambiguity at the tactical level"[93] as to

---

89 In May 2016 the European Council formally adopted new rules to step up the security of network and information systems across the EU under a network and information security (NIS) directive. The strategy has five priority areas: achieving cyber resilience; drastically reducing cybercrime; developing cyber defence policy and capabilities related to the EU's common security and defence policy (CSDP); developing the industrial and technological resources for cyber security; establishing a coherent international cyberspace policy for the EU.

90 Located in Victoria, London the Centre has a team of around 700 staff.

91 Ciaran Martin, formerly Director General for cyber security at the UK Government Communications Headquarters (GCHQ), inaugural Head of the UK National Cyber Security Centre.

92 The NCSC has not publicly defined what it means by taking "specific action" with industry to address large-scale, non-sophisticated

cyberattacks. The full range of "active defence" measures goes from low risk information sharing to more extreme botnet takedowns and

white-hat ransomware retaliatory cyberattacks.

93 Center for Cyber & Homeland Security, The George Washington University (Project Report October 2016) Into the Gray Zone –

what is legally permissible. Commenting on their Report the Associate Director CCHS and the Report's Policy Analyst noted, "until significant consequences are visited upon perpetrators of threats there will be little incentive for them to change their ways. On the other hand, vigilantism, with the potential for expansive collateral damage, is not the answer[94]". The current failure of international law to address the core legal principles which should govern "active defence", the legal right to bare cyberarms if you will[95], is no longer sustainable in a situation where the status quo favours no one more than the cyberattacker.

The Private Sector and Active Defense Against Cyber Threats 45.

94 IPI Global Observatory Sharon L. Cardish and Taylor P. Brooks, Mounting an Active Defense Against

Cyber Threats, (10th November 2016) 2.

95 See the prposed Active Cyber Defense Certainty Act, a draft US Bill to amend section 1030 of the Computer Fraud and Abuse Act giving

private victims a retaliatory legal right to hack back their attacker, subject to prior notification of the FBI and avoiding the destruction of

data on third party~~'s~~ networks or computers.