INTELLECTUAL PROPERTY AND NATIONAL SECURITY

(Accepted article version, Journal of Intellectual Property Law and Practice, 24 October 2016)

Marta Iljadica and Paul F Scott*

1. INTRODUCTION

In the United Kingdom, the security services (by which we mean the Security Service (MI5), the Secret Intelligence Service (MI6) and the Government Communication Headquarters (GCHQ)) enjoy statutory powers of property interference to be made use of in pursuing the functions identified for them by statute.[1] A recent judgment of the Investigatory Powers Tribunal (the body charged with adjudicating upon, amongst other things, human rights claims against the security services)[2] relating to the use of those powers for 'computer network exploitation' (hacking) provides important insight into the place of intellectual property within the matrix of these national security powers. The present article takes its lead from the decision of the IPT in that case, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and the Government Communications Headquarters*,[3] focussing on those observations within it relating specifically to intellectual property. In its first part, the article extrapolates from what is said (and left unsaid) in that judgment in order to discuss the ways in which intellectual property rights might be lawfully over-ridden or limited in pursuit of national security objectives. It then, in its second part, expands out to consider other ways in which the ordinary operation of the regime of intellectual property rights may be modified in light of the exigencies of national security. Given the extent to which threats to national security, and state responses to it, take place upon a technical plane, both of these questions are of great – and growing – significance. Consideration of them here suggests that the landscape of intellectual property law incorporates the exigencies of national security to a far greater extent than has hitherto been appreciated, but that the confirmation by the IPT of the possibility of using the Intelligence Services Act 1994 (ISA 1994) to authorise the infringement of intellectual property rights is likely to ensure (if it was not already the case) that the 1994 Act is the favoured mechanism of those called upon to protect the UK's national security.

---

* Lecturer in Law, University of Southampton, Lecturer in Public Law, University of Glasgow. We are grateful to the anonymous reviewer for very helpful comments on an earlier draft.

[1] See Intelligence Services Act 1994, s 5(2)(s) referring to the functions of the Security Service in the Security Service Act 1989; the Secret Intelligence Service's functions in ISA 1994, s 1; and those of GCHQ in ISA 1994, s 3.

[2] See Regulation of Investigatory Powers Act 2000, ss 65-70.

[3] [2016] UKIP Trib 14_85-CH. The Privacy International case (Case No. IPT 14/85/CH) was joined by that of Greennet Limited and six other claimants against the same respondents (Case No. IPT 14/120-126/CH).

2. INTERFERENCE WITH INTELLECTUAL PROPERTY UNDER ISA 1994

The IPT judgment considers copyright in the context of hacking and the statutory power of property interference. In this part we address the IPT's assessment of the applicability of section 5 ISA 1994 warrants to intellectual property. The operation of section 50 Copyright Designs and Patents Act 1988 (CDPA) and the relevance of the Infosoc Directive and licensing agreements, both of which are briefly mentioned by the IPT are discussed in subsequent sections below. Although it was not addressed by the IPT, we also consider the possibility of a distinct public interest defence to claims of copyright infringement where the underlying act is carried out in pursuit of national security interests.

a. Copyright in the IPT's judgment

The Secretary of State is empowered, by section 5 ISA 1994, to issue warrants which authorise 'the taking… of such action as is specified in the warrant in respect of any property so specified'. The conditions under which this power may be exercised include that the Secretary of State thinks it 'necessary for the action to be taken for the purpose of assisting' the security services to carry out the functions assigned to them by statute – either ISA 1994 in the case of MI6 and GCHQ, or the Security Service Act 1989 in the case of MI5. The functions of MI5 include 'the protection of national security and, in particular, its protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means'[4] and the safeguarding of 'the economic well-being of the United Kingdom against threats posed by the actions or intentions of persons outside the British Islands'.[5] Those of MI6 and GCHQ are more generic and more specialised respectively, but in each case may be exercised only in the interests of national security 'with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom', in the interests of the United Kingdom's economic well-being, and in support of the prevention and detection of serious crime.[6] Further, the action taken must be proportionate to what it seeks to achieve,[7] and suitable arrangements must (as demanded by the relevant statutes) be in place to prevent the unauthorised disclosure of information obtained via use of these powers.[8] Section 5 ISA 1994 provides explicitly that '[n]o entry on or interference with property or with wireless telegraphy

[4] Security Service Act 1989, s 1(2).
[5] Security Service Act 1989, s 1(3).
[6] Security Service Act 1989, s 1(4).
[7] Intelligence Services Act 1994, s 2(b).
[8] Intelligence Services Act 1994, s 2(c).

shall be unlawful if it is authorised by a warrant issued by the Secretary of State under this section.'[9]

The specific issue of interference with intellectual property arose in *Privacy International* in the context of a challenge to the use of these powers of property interference to carry out 'computer network exploitation' (CNE) – more usually described simply as (computer) hacking – brought by lobby group Privacy International and a number of small Internet Service Providers. One issue on which the IPT was required to rule was the question of whether or not the statutory authority permitted interferences with 'intangible legal rights',[10] exemplified here by – but undoubtedly not limited to – copyright. In line with the argument of the claimants, one might distinguish between 'pure' interferences with intellectual property and those which are a necessary consequence of a primary interference with physical property. The distinction is that the latter can be presumed to be implicitly authorised by a section 5 warrant, even if the reference to 'property' in section 5 is taken to apply only to real property. 'Pure' intellectual property interference can be authorised, however, only if 'property' in the ISA 1994 is understood to include intellectual property. Examples of the sort of 'pure' property interference at issue given in a leaked GCHQ request for the renewal of an ISA warrant include 'modifying commercially available software to enable interception, decryption and other related tasks',[11] as well as the reverse engineering of software products where these things are done not as a preparatory step towards a specific act of property interference but are carried out instead 'as part of GCHQ's continuing efforts to maintain its technical knowledge base and develop future exploitation opportunities.'[12] These acts, the renewal request suggests, 'may represent an infringement of copyright'[13] and it is for that reason that the question arises.

That copyright is 'property' is made clear in section 1(1) CDPA: copyright is 'a property right' subsisting in, amongst other things, literary works[14] which are further defined to include computer programs.[15] In the request for the renewal of a warrant permitting such activities, it was observed that when the warrant in question had originally been issued, 'there was believed to be no precedent for the use of a warrant under section 5 of ISA 1994 in relation to intellectual

[9] Intelligence Services Act 1994, s 5(1).
[10] *Privacy International*, [24].
[11] GCHQ Application for Renewal of Warrant GPW/1160 (13 June 2008) [4]. The warrant renewal request was leaked by Edward Snowden to *The Intercept* and can be found at: [https://theintercept.com/document/2015/06/22/gchq-warrant-renewal]. For discussion, see A Fishman and M Marquis-Boire, 'Popular Security Software Came Under Relentless NSA and GCHQ Attacks', 22 June 2015, [https://theintercept.com/2015/06/22/nsa-gchq-targeted-kaspersky/].
[12] *Ibid*, [5].
[13] *Ibid*, [4].
[14] CDPA, s 1(1)(a).
[15] CDPA, s 3(1)(b).

property as embodied in copyright or licensing agreements.'[16] The request stated, however, that the Intelligence Services Commissioner had been consulted (in 2005) and been 'content'[17] that section 5 could be used to remove liability which might otherwise arise out of such activity. Similarly, a more recent report of the Intelligence Services Commissioner states clearly, but does not elaborate, that with respect to section 5 ISA and warrants issued under it '[p]roperty includes physical property and intellectual property.'[18] Before the IPT, the primary argument advanced in favour of the proposition that this was incorrect – that 'property' in the 1994 Act does not, properly understood, include intellectual property – was that the provision permitting interference with property differs in its effect as regards 'property in the British Islands',[19] indicating (it was argued) that intellectual property could not be included within the property interferences with which were foreseen by the provision. The IPT made short work of this submission, noting (most relevantly for present purposes) 'that as defined by statute copyright is a collection of rights in respect of the United Kingdom'.[20] Even accepting the correctness of this conclusion, this would seem to leave certain of the issues arising out of this question of location unaddressed. Because certain interferences are, under the statutory framework, disallowed if the property being interfered with is 'in the British Islands',[21] it becomes necessary to understand where intellectual property is located, and whether or not an act done to physical property abroad might constitute an interference with an intangible property right which is 'located' in the United Kingdom (and, in turn, what that means for the legality of the underlying interference with physical property). This difficulty is less likely to arise in relation to 'pure' intellectual property rights. That is, where the security services are reverse engineering software,[22] it is likely that the IP rights interfered with are 'in the British Islands' in all relevant senses and so the statutory distinction between interferences within and outside of the British Islands does not become relevant. Nevertheless, the conclusion that copyright (and also, presumably, other intellectual property rights interference with which might be authorised) arises in the United

[16] GCHQ Application for Renewal of Warrant GPW/1160 (13 June 2008) [17].
[17] *Ibid.*
[18] M Waller, *Report of the Intelligence Services Commissioner for 2014* (2014) HC 225 SG/2015/74, 17.
[19] ISA 1994, s 5(3) and s 5(3A). The distinction is this: such property can be interfered with by MI6 and GCHQ for reasons of national security and the protection of the UK's economic well-being, but not for purposes of preventing and detecting serious crime; MI5, alternatively, may interfere with property in the UK for such reasons, though under a particular definition of serious crime.
[20] *Privacy International*, [26].
[21] ISA 1994, s 5(3) and s 5(3A.
[22] The decompilation exception in s 50B CDPA would not seem to apply here nor can the security services' interference fall within the ambit of observation, study or testing of a computer program in s 50BA CDPA. The issues raised by the reverse engineering of computer programs are made more complex insofar as such acts may reveal confidential information which presents another (potential) property interference. See T Aplin, 'Reverse Engineering and Commercial Secrets' (2013) 66 CLP 341. Decryption of information may be a copyright infringement or a database right infringement but not necessarily a breach of confidence. See on this point *Mars UK Ltd v Teknowledge Ltd* [2000] ECDR 99, and T Aplin et al, *Gurry on Breach of Confidence* (OUP 2012), §5.34.

Kingdom implies that certain of the powers existing under the ISA 1994 (which do not extend to the British Islands) are not available in relation to it. The IPT's treatment of the matter is from this point of view unfortunately brief, focussed only upon resolving the minimum of the legal dispute before it.

The question of the scope of 'property' leads directly to the concept of interference, and the concept of what differentiates such a thing from, say, a mere use, or other interaction. Much of the difficulty in addressing this point with any specificity arises from the fact that it is not clear in the judgment of the IPT what exactly is the nature of the relevant actions carried out by the security services which (actually or potentially) constitute an interference with intangible rights. In the realm of physical property, with which the common law's commitment to the rule of law in the form of a requirement of legality is normally concerned in the first place, the question is usually answered via concepts of tort – usually that of trespass, but presumably also statutory torts including that of wrongful interference with goods.[23] This reflects the idea – to which the key case in this area attests – that where there is no wrong involved, what we are dealing with is not an interference. And only if there is such an interference – the common law constitution says – is authority is required for the act, whether act is perpetrated by a public or a private actor.[24] In the realm of intellectual property, the concept of interference can be assimilated with that of an infringement. That is, an interference with intellectual property for which authority is required would seem to occur only insofar as the act in question was a breach of copyright (for example, the reproduction of a copyright protected work).[25] Merely accessing a computer program does not infringe any of the author's economic rights and so such access is not wrongful – in other words, it would not constitute an interference with a property right – and so no authority would be required for the state to do so. Thus, while all infringements of copyright will (where there is not some supervening defence) be an interference for which authority is required,[26] there remain a vast range of 'uses' of such work which do not constitute interferences and for which neither the 1994 Act nor other authority need be prayed in aid. Nevertheless, a given act might constitute an interference notwithstanding that from many points of view the intangible right interfered with remains intact; as such, that the copyright owner's rights as against third-parties survive any interference with copyright by the security services is not relevant to the act's

[23] See eg *Entick v Carrington* (1765) 29 St Tr 1029.
[24] *Malone v Metropolitan Police Commissioner (no 2)* [1979] Ch 344.
[25] Relevant parts of the Equipment Interference Code of Practice give some indication of how information obtained by hacking might be used – including copied, and disseminated – which potentially overlaps with the economic rights of a copyright owner. See *Privacy International*, Appendix II.
[26] The court in *Ashdown* is clear that 'The infringement of copyright constitutes interference with "the peaceful enjoyment of possessions"…' at [28] (Phillips MR). Note that the CDPA makes the *infringement of copyright* actionable and makes the same remedies available as those for the 'infringement of any other property right' CDPA, s 96(2).

wrongful status, nor the requirement of authority which follows from it. The essential point is that a given act is to be an interference with copyright which must be authorised by some legal rule (in this case, section 5 ISA 1994) would require demonstrating that the copyright owner's exclusive economic rights[27] have been infringed by the particular act at issue,[28] such that the act was an interference with a property right.

A further question is whether, if the access of a computer programme requires the circumvention of a 'technical device',[29] such act will be an interference with property which must be (and, indeed, can be) authorised by a warrant under section 5 ISA 1994. One relevant provision of the CDPA seeks to prevent the sale of 'means' which have as their 'sole intended purpose' the removal or circumvention of such devices (or the publication of information intended to enable such removal or circumvention) where the seller or publisher knows or has reason to believe that the 'means' or the information 'will be used to make infringing copies'.[30] Neither of these acts would seem likely to be amongst practices of the security or other services in the course of investigations for national security purposes: the most likely related possibility is the sharing of information that is designed to assist partner agencies in circumventing technical measures, but this would not seem to count as publication.[31] With respect to works other than computer programs, the protection offered is more expansive with section 296ZA providing that where a person knowingly[32] circumvents a 'technological measure' the copyright owner or the exclusive licensee will 'have the same rights against [the person circumventing] as a copyright owner has in respect of an infringement of copyright'.[33] This applies even – it would seem – if the circumventer does not know (and has no reason to believe) that it will be used to make infringing copies. Nevertheless, the provision does not seem to explicitly constitute the circumvention as a breach of copyright, but simply provides for the existence of 'the same rights' where such circumvention takes place. As such, it cannot be said with certainty that the circumvention of protection measures is a property interference for which authority must be sought. If it is not, a potentially important lacuna has been left in the system by which copyright works are protected.

---

[27] eg right to reproduce the work in s 17 CDPA, right to communicate the work to the public in s 18 CDPA.
[28] Copying a work without the permission of the copyright owner is prohibited: CDPA, s 17(2). It is unclear whether hacking itself would result in the computer program (as a literary work) being 'stor[ed]… by electronic means'.
[29] A separate protection scheme exists for computer programs in s 296 CDPA which is rather more limited than that protection other forms of authorial works.
[30] CDPA, s 296.
[31] Note that elsewhere in the CDPA 'publication' is defined to mean the 'issue of copies to the public': CDPA, s 175(1)(a).
[32] CDPA, s 296ZA(1).
[33] CDPA, s 296ZA(3).

b. Issues beyond the IPT's judgment

The IPT judgment offers a hint of another potential avenue for accommodating national security concerns within the copyright framework, in noting that counsel for the claimants had raised (but did not pursue) the implications of the Infosoc Directive.[34] No further indication is given as to what the argument would have been. The relevant Skeleton Argument, reproduced on Privacy International's website,[35] suggests that the claimant's argument was based on the proper interpretation of the 'public security' copyright exceptions in light of the Directive's three-step test. The exception in the (exhaustive but not mandatory) list in the Directive that was highlighted here was the text in Article 5(3)(e): 'use for the purposes of public security or to ensure the proper performance or reporting of administrative, parliamentary or judicial proceedings'. The exception must be viewed in the context of recital 34 of the Infosoc Directive whereby EU Member States may include a 'public security' limitation or exception.[36] The reference to 'public security', however, was merely mentioned in the Skeleton Argument in the context of the reverse engineering of software, 'presumably with a view to developing malware'.[37] Specifically, the claim was that reverse engineering of software did not meet the three-step test in Article 5(5) of the Directive because it would conflict with the relevant works' normal exploitation, therefore ensuring that the alleged infringer could not take advantage of the security exception. Whether or not it is correct that a UK court must address the three-step test directly,[38] it seems that the existence of a power to interfere with copyright for national security purposes would nevertheless be compatible with the Directive: Article 9 provides that the Directive is, amongst other areas of law, 'without prejudice to provisions concerning… security', a formulation which would encompass warrants issued under section 5 ISA 1994.[39] Consideration of the Infosec Directive therefore seems to add nothing to the question viewed solely as a matter of domestic law. The claimants were correct not to press the point.

The IPT's judgment does not address the implications of the ECHR for the question of interference with intellectual property rights (though much of it is concerned with the Article 8

[34] 'An argument in relation to the possible impact of the EU Copyright Directive (2001/29/EC), raised by Mr Jaffey in his pleadings and his skeleton argument, was not pursued': *Privacy International*, [29].
[35] Made available at [https://www.privacyinternational.org/sites/default/files/PI_Greennet_Skeleton_FINAL.pdf]
[36] Recital 51 of the Directive also refers to 'public security' in the context of technological protection measures. See also, regarding databases, the more general exception akin to s 50 CDPA in para 6 Copyright and Rights in Databases Regulations 1997/3032 providing an exception to copyright in databases for the purpose of public administration. See also Article 6(2)(c) Directive 96/9 on the legal protection of databases, OJ L 77, 20–28.
[37] Skeleton Argument, 25 November 2015, Ben Jaffey and Tom Cleaver (Blackstone Chambers), [42].
[38] See, arguing that in light of recent CJEU case law national courts are required to assess whether an particular national exception meets the three-step test, R Arnold and E Rosati, 'Are National Courts the Addressees of the InfoSoc Three-Step Test?' (2015) 10(10) JIPLP 741.
[39] Note also that this security exception may be tied to ss 45-47 CDPA: S Stokes, 'The UK Implementation of the Information Society Directive: Current Issues and Some Guidance for Business' (2004) 10 CTLR 5, 9.

implications of CNE as a form of property interference generally). The right to peaceful enjoyment of one's possessions is protected by Article 1 of the First Protocol to the Convention (A1P1), and intellectual property can certainly be such a possession, [40] having the economic value which the Court of Human Rights in Strasbourg has placed at the heart of that concept. The interference with intellectual property would, in turn, undoubtedly constitute 'control' (rather than deprivation)[41] of one's possession. Nevertheless, both the plain text of the Convention and the (not wholly equivalent)[42] interpretation given to it by the Strasbourg court are relatively generous in the conditions they create for the justification of any such control. For present purposes, it suffices to note that paragraph 2 of A1P1 explicitly permits parties to the Convention to 'enforce such laws as it deems necessary to control the use of property in accordance with the general interest', a formulation which would undoubtedly include laws (such as ISA 1994) enacted to promote the interests (or, if they are not the same thing, the apprehended interests) of national security. Though the question of the proportionality of a particular interference is of course fact-sensitive, any court determining the issue would be slow to disagree – in this most sensitive of contexts – with the assessment of the political decision-maker. This conclusion applies also to those other forms of intangible property, discussed below, interference with which would seem to be similarly possible under a section 5 ISA warrant.

c. Other IP rights

The basic conclusion of the IPT has implications for other intangible rights, such as patents, designs and registered trade marks,[43] all of which are property rights and so might be infringed under the authority of a lawfully-issued section 5 ISA 1994 warrant (even if the necessity of interfering with trade marks and designs for national security purposes may seem less likely). A further question of interest here, however, is whether the *information* accessed by GCHQ through hacking is (or might under certain circumstances be treated as) property. This question is important because of the possibility that in at least some contexts, the acquisition of information via hacking will be a tortious act – whether breach of confidence or the misuse of private information – for which legal authority is required. If it is not the case, however, that information is property, then that prima facie tort cannot be directly authorised by a warrant under section 5 ISA 1994; if authorised at all, it must be so because it is a necessary incident of

[40] See, eg, *Smith Kline and French Laboratories Ltd v The Netherlands* (1990) 66 DR 70 regarding a patent.
[41] ECHR, Article 1 Protocol 1(2).
[42] See *Sporrong and Lönnroth v Sweden* (1983) 5 EHRR 35.
[43] Patents Act 1977, s 30(1); CDPA, s 213(1); Registered Designs Act 1949, s 7(1) (referring to the 'registered proprietor'), s 19 (referring to the possibility of mortgaging a registered design), and (the repealed) s 19(4) (referring to the registered design in the context of assignment as being 'like… any other personal property' indicating that a registered design right was to be treated as property); Trade Marks Act 1994, s 2(1).

an authorised and therefore lawful interference either with physical or intellectual property. This potentially becomes relevant, in turn, where there is a temporal separation between the original act of property interference authorised in a warrant and the consequent acquisition or communication of confidential information facilitated by that act. In short, section 5 ISA 1994 authorises interferences with property and yet the status of confidential information, indeed any information, *as property* is uncertain. The relevant Strasbourg and English case law indicates that confidential information is property on the basis of having an economic value.[44] Yet as Aplin argues, confidential information is not like other forms of intellectual property: for example 'there are weak grounds to classify trade secrets as a 'possession' on the basis of its transferability'.[45] Tellingly, the EU Trade Secrets Directive requires Member States to protect such information without requiring the protection to take the form of a property right.[46] If, however, confidential information *is* property, the implication of the IPT judgment is that it would apply to confidential information in the same way as to other intangible property, that is, that such interference could be authorised by a warrant under section 5 ISA 1994.[47]

Furthermore, a distinction must be drawn between merely accessing information and disclosing that information to others. As Aplin argues, by reference to dicta in *Hellewell v Chief Constable of Derbyshire*,[48] it is the *disclosure* of information that would give rise to a breach of confidence.[49] The issue as it relates to investigations of a national security nature is that insofar as confidential information is interfered with, it is not likely to be disclosed in the manner of the 'mugshot' in *Hellewell*, as doing so would be likely to be in breach of the arrangements which ISA 1994 (and its 1989 predecessor) require to be put in place and to which the Secretary of State must be satisfied that any information obtained via property interference will be subject.[50] It is likely in any event that in the case of disclosure, a public interest defence would be available,[51] particularly if that disclosure takes place in accordance with the relevant statutory limitations, which tie permissible disclosure to the statutory functions of the security services. In light of the relevant case law, it is also clear that photographs taken in secret, for instance would not in and of themselves

[44] See generally LR Helfer, 'The New Innovation Frontier? Intellectual Property and the European Court of Human Rights' (2008) 49 Harv L Rev 1.
[45] T Aplin, 'Right to property and trade secrets' in C Geiger (ed) *Research Handbook on Human Rights and Intellectual Property* (Edward Elgar 2015), 424 (footnotes omitted).
[46] T Aplin, 'A Critical Evaluation of the Proposed EU Trade Secrets Directive' (2014) 4 IPQ 257, 260.
[47] It follows that the tort of misuse of private information would also be excused: *Vidal-Hall v Google* [2015] FSR 25 The same may well apply to the tort of trespass.
[48] [1995] 1 WLR. 804, 807.
[49] Aplin, 'Reverse Engineering and Commercial Secrets', 361.
[50] Security Service Act 1989, s 2(2)(a); Intelligence Services Act 1994, s 2(2)(a), s 4(2)(a), and s 5(2)(c).
[51] See *Hellewell v Chief Constable of Derbyshire* [1995] 1 W.L.R. 804, 807.

constitute a misuse of private information.[52] This means that there will in many cases be, at the precise point at which information is accessed via hacking, no tortious act which requires authorisation under a section 5 warrant. Even where there is a requirement for such authorisation, however, it is likely to be considered to be provided by the underlying warrant justifying the relevant interference with physical property.[53] Finally, while trade secrets may or may not attract A1P1 protection as possessions,[54] confidential information (where personal or private) may also be protected by Article 8 ECHR. Given, however, that the conditions of justified interference are broadly equivalent, there is likely to be no issue in terms of the justification available for the interference.

3. OTHER AVENUES RELEVANT TO NATIONAL SECURITY INFRINGEMENT

In this section we consider other legal rules which may have a parallel effect to the use of a section 5 warrant, and discuss the reasons for which the ISA 1994 will be preferred, where it is available to use.

a. The (ir)relevance of section 50 CDPA

In finding that section 5 ISA 1994 enabled interference with intangible property– whether or not such interference was ancillary to an interference with tangible property – the IPT states that that '[a] s.5 warrant is as sufficient authority for such interference as is s.50 of the Copyright Designs and Patents Act 1988'.[55] That section provides that '[w]here the doing of a particular act is specifically authorised by an Act of Parliament, whenever passed, then, unless the Act provides otherwise, the doing of that act does not infringe copyright.'[56] Parliamentary debate at the time of the enactment of the CDPA indicated that '[t]he exception in Clause 50 is intended to apply only when some particular act is authorised by an Act of Parliament.'[57] Two points can be made about this provision. The first is that – if the IPT intends section 50 to buttress its prior conclusion, that intellectual property is property of a kind with which interference may be authorised under a section 5 ISA 1994 warrant – it is unclear exactly what work section 50 CDPA does in providing authorisation for the infringement of copyright. That is, the IPT fails to consider the specific terms of the provision and, in particular, the reference to an act being

[52] *Ibid*, referring to cases including *Mosley v News Group Newspapers Ltd* [2008] EMLR 20.
[53] Furthermore, the disclosure of information possessed by members or former members by the security services by virtue of their status as such is disallowed by Official Secrets Act 1989, s 1(1). See generally T Aplin et al, *Gurry on Breach of Confidence* §13.68.
[54] On which see T Aplin, 'Confidential Information as Property?' (2013) 24 KLJ 172, 172.
[55] *Privacy InternationalI,* [28].
[56] Subsection 3 provides further reassurance: 'Nothing in this section shall be construed as excluding any defence of statutory authority otherwise available under or by virtue of any enactment'
[57] Hansard, HL vol 495, col 643.

'*specifically* authorised' (emphasis added). It seems too great a stretch to suggest either that interference with intellectual property is *specifically* authorised by section 5 (which is of course not the same as suggesting that it is not, contrary to the IPT's conclusion, authorised at all) or that any particular interference carried out under a warrant issued under that provision is *specifically* authorised by it. If the invocation of section 50 CDPA is intended to reaffirm the original conclusion, it does not make any useful contribution to doing so.

More generally, however, on a careful consideration of its terms, we see that section 50 CDPA has no legal effect of its own. It simply recognises the basic truth that legal rights encompass correlative legal relations – explicitly permitting one party to do a certain act is logically incompatible with any other party having the power to stop that act being done. The relevant 'act' must either be authorised by statute (section 50(1) CDPA) or under some other 'defence of statutory authority otherwise available under or by virtue of any enactment' (section 50(3) CDPA). That is, section 50(1) CDPA does not itself authorise anything, but merely makes provision as to the effect of acts authorised elsewhere on the statute book. This is particularly important in light of the fact that, on the best reading of the IPT's judgment, it identifies section 50 not as confirming the correctness of its conclusion as to the effect of the 1994 Act, but instead as providing a parallel basis of lawful interference with copyright ('[a] s.5 warrant is as sufficient authority for such interference *as is* s.50 of the Copyright Designs and Patents Act 1988').[58] It does not do so because, only recognising the effect of authority found elsewhere, it cannot provide authority for anything not otherwise authorised. The invocation of section 50 CDPA here is therefore doubly vacuous and the better view must be that a lawfully issued section 5 ISA 1994 warrant would suffice to ensure that any interference with a relevant 'work' carried out under it would not constitute an infringement of copyright, *whether or not* the possibility of statutorily authorised interference was recognised by the terms of the CDPA. This view is supported in *Copinger*, which notes that the inclusion of section 50 in the CDPA was unnecessary given that with a statutory authority defence it always would have been the case that an infringement specifically authorised in another statute would have the effect of providing a defence to copyright infringement.[59] This redundancy of section 50 has important implications for interferences with other forms of intellectual property rights such as patent, design, and trade mark rights, and rights relating to confidential information, where – even in the absence of a provision equivalent to section 50 CDPA – otherwise infringing acts will be lawful if done in

[58] Emphasis added.

[59] *Copinger and Skone James on Copyright* (17th ed) [9-224] pointing also to s 50(3) CDPA which provides that 'Nothing in this section shall be construed as excluding any defence of statutory authority otherwise available under or by virtue of any enactment.'

accordance with a section 5 warrant. This is not to say that section 50 is entirely without significance; in particular, it is likely to be helpful in countering any argument that the enactment of the CDPA impliedly repealed powers of interference with copyright contained within statutes enacted prior to the CDPA itself. Its inclusion can for that reason be seen as – if nothing else – confirming that such powers persist notwithstanding the new statutory framework for copyright.

Finally, and putting this apparent redundancy to one side temporarily, the ambit of section 50 remains unclear as, apart from the IPT judgment under discussion here (which does not elaborate on the alleged ability of the provision to constitute authority for a breach of copyright), the issue of 'statutory authority' does not seem to have been considered elsewhere in the copyright case law. Indeed there is very limited discussion of section 50 in the legal literature generally. One exception is a study of freedom of information, which identifies copyright as a potential obstacle to responding to FOI requests because to respond would require the copying of the requested documents.[60] The argument made is that the Freedom of Information Act 2000 (FOIA) must authorise the copying of documents (in the manner foreseen by section 50) because to do otherwise would prevent that statute from operating as intended.[61] This argument may be undermined in part by the reference that the 2000 Act makes – in sections 11A, 11B and 19 – to the use to which copyright-protected material released thereunder may be put[62] (in the sense that the specific provision undermines any claim that there exist implied rules of a broader scope). It nevertheless remains true that in some cases, material which the relevant public authority (as opposed to the party to whom it is released, with whose use of the material sections 11A, 11B and 19 is concerned) might be required to release in accordance with the FOIA could not be released if to copy that material was not taken to be permitted by the 2000 Act. And, with respect to the specific issue of copyright infringement for national security ends, the lack of engagement with section 50 CDPA in the case law and academic literature might be explained by the nature of national security investigations themselves. The relevant acts, such as the CNE under consideration in *Privacy International*, are unlikely either to affect the market for a copyright protected work or to come to the attention of a person with the capacity and will to challenge the legality of what may be a prima facie breach of their intellectual property rights.

b. National security and Crown use of patents

[60] J Apostle and M Lawry, 'Could Copyright Be an Obstacle to an Efficient and Effective Freedom of Information Regime?' (2005) 1(4) Freedom of Information 3.
[61] *Ibid*, 6.
[62] The sections concern datasets, fees for the use of data sets and publication schemes respectively. Note that s 80(3) FOIA refers specifically to s 50 CDPA in order to make clear that s 50 applies *also* to the Freedom of Information (Scotland) Act 2002. However, this, like s 50 itself, would seem to be redundant.

The Patents Act 1977 (PA 1977) makes provision as to the use of patented inventions by the Crown that would – although national security is not explicitly referred to – be likely to offer a defence to any patent infringements occurring as part of the intelligence services' counter-terrorism work.[63] A contrast, though, can be drawn between section 50 CDPA and the most relevant provision, section 55, of the PA 1977.[64] Where section 50 CDPA appears to be redundant, section 55 PA 1977 does offer an alternative ground on which to defend property interference as it relates to patented inventions. It provides that a government department (or a person 'authorised in writing by a government department')[65] may, for example, use an invention without the patent owner's consent – something which would otherwise be an infringement of that person's rights.[66] This provision is potentially relevant to the kinds of national security operations under discussion here. Though the security services are not part of any government department, they operate under the authority of the Home Secretary (in MI5's case) and the Foreign Secretary (in MI6 and GCHQ's case) and so might plausibly be 'authorised' by the departments headed by those persons.[67]

A potential difficulty presents itself in relation to whether national security purposes are of a kind covered by the provision, and if so what limits might exist upon the Crown's use of patented inventions. Section 56 PA 1977 relates to the interpretation of the terms of Crown use and, for our purposes, identifies as part of 'the services of the Crown', 'the supply of anything for foreign defence purposes' in section 56(2)(a) PA 1977. It is not immediately clear that this would cover use for purposes associated with internal security; this would appear to be a foreign defence purpose in a very attenuated form, and in any event section 56(3) PA 1977 defines 'foreign defence' narrowly.[68] However, the relevant provision does not claim to be exhaustive, but merely 'includes' foreign defence as a relevant service.[69] Better, therefore, to read that provision as intended to dispel any doubts about whether foreign defence falls within 'the services of the Crown' and as therefore representing a tacit acceptance that domestic national security endeavors would undoubtedly do so. The case law offers relatively little guidance on this issue, with much of it concerned with disputes over pharmaceuticals and public health, and even then

[63] We do not suggest that CNE at issue would have in question would have constituted a patent infringement or patent infringements. In particular, computer programs are not patentable subject matter: PA 1977, s 1(2)(c).
[64] Amongst other relevant sections 'Crown use' is covered in ss 55 - 59 PA 1977.
[65] PA1977, s 55(1).
[66] PA 1977, s 60(1).
[67] See *MMI Research Ltd v Cellxion Ltd* [2009] EWHC 1533 (Pat), [4]-[12] where it was accepted (contrary to what had been claimed by the defendants in their skeleton arguments) that a police force was not a government department and so could only make use of the relevant intention if it had been authorised to do so (which it had not).
[68] Referring specifically to the 'sale or supply' to a foreign government or pursuant to a United Nations resolution.
[69] This point is also highlighted in Intellectual Property Office, *Manual of Patent Practice*, version published July 2016 at [56.03]. Note also the more generous provisions for Crown use in a 'period of emergency': PA 1977, s 59.

infrequently.[70] Therefore, assuming a product or process is 'used' for national security purposes, it would be highly likely – if suitably authorised – to fall within the scope of Crown use, and consent would not need to be sought in respect of any uses of patented inventions by the intelligence services. The use would in those circumstances not constitute property interference of a sort requiring distinct authorisation under section 5 ISA.

Two other points are of relevance here. The first is that of compensation. Assuming national security use by the intelligence services is Crown use under section 55 PA 1997, the question remains as to whether compensation may be sought by the proprietor of the patent. In *Henry Brothers (Magherafelt) Ltd v Ministry of Defence*[71] – regarding co-ownership and the revocation of a patent for a prefabricated, bomb-proof building – this question was considered and the plaintiff, as (alleged) co-owner of the patent, was denied compensation for the invention's use because the Crown was in fact the owner of the patent in question.[72] Where ownership is not in dispute, and the invention has not been previously 'recorded or tried' by the government department, then section 55(4) requires that terms be agreed with the patent proprietor and approved by the Treasury.[73] A second, and prior, question is whether the use of the invention would come to the attention of the proprietor at all. Section 55(7) PA 1977 requires the owner of the patent that is being used by the Crown under that provision to be notified of its use, either 'as soon as practicable' after use or after the grant of the patent, if use begins before then.[74] However, this requirement of notification is subject to an exception in circumstances in which 'it appears to the department that it would be contrary to the public interest to do so'.[75] Maintaining secrecy of such use on national security grounds would undoubtedly be a matter of significant public interest – since to notify of a use may reveal aspects of security service operations[76] – thus obviating the need for notification and (in turn, and more problematically) any compensation which may be required to be paid to the owner for the use being made of the invention.[77] In any event, insofar as the 1994 Act offers a means by which to justify interference with a patent (including, for present purposes, unlicensed use of the patented invention) – as the decision in

[70] See eg *Dory v Sheffield HA* [1991] FSR 221.
[71] [1997] RPC 693 – in the Patents Court, claim for compensation dismissed.
[72] [1997] RPC 693, 718. The matter arose on appeal with respect to section 58(1) PA 1977: *Henry Brothers (Magherafelt) Ltd v Ministry of Defence and Northern Ireland Office* [1999] RPC 442. The appeal was not successful.
[73] Disputes as to terms may be referred to the court: PA 1977, s 58(1)(b).
[74] See also PA 1977, s 55(7).
[75] The subsection continues that this is to occur 'as soon as practicable after the second of the following events, that is to say, the use is begun and the patent is granted, and furnish him with such information as to the extent of the use as he may from time to time require.'
[76] Or, though it is not the focus of the present work, military operations.
[77] ie in the setting of agreed terms: PA 1977, s 55(4). Note however that compensation does not need to be provided in certain cases, namely the recording of the invention by the government department before its priority date: PA 1977, s 55(3).

Privacy International would seem to demonstrate is possible – there exists a method by which the security services might evade any and all requirements of notification and compensation, for neither of which ISA 1994 makes provision. Whether the preference of the security services is to avail themselves of an authorisation under the PA 1977 or a warrant under ISA 1994 is of course difficult to know. No figures seem to exist as to the number of such authorisations issued and details as to ISA warrants are only given at a level of generality that makes it impossible to know how many might be granted relating to intellectual property. Nevertheless, on consideration of the relevant statutory frameworks, we see that there are compelling reasons for which the security services will prefer, if at all possible, to make use of the authority of the 1994 Act, leaving the specific provisions of the PA 1977 to actors - the police may be one example - who cannot avail themselves of the ISA's broad powers, or for situations in which the requirements of the 1994 Act are not met.

c. National security and Crown use of designs

As is the case with patents, specific exceptions to rules regarding infringement exist for Crown use of UK unregistered designs. The relevant provision is found in section 240(1) CDPA, which enables a government department (or an individual so authorised, again allowing the security services to benefit from them) to supply and dispose of articles 'for the services of the Crown'. Unlike in the PA 1977, the definition of 'Crown use' offered here is exhaustive, but also unlike the PA 1977, national security can be easily read as a permitted Crown use, section 240(2)(a) listing 'defence of the realm'[78] – the historically preferred legal phrasing – as a relevant service of the Crown. Where use of a design that would otherwise be infringing is made, section 241 CDPA requires setting of terms for the use of the design but, again, the relevant department may elect not to do so where it 'appears to the department it would be contrary to the public interest'. The public interest here, as with patented inventions, might easily be interpreted so as to include national security concerns. Yet it is unclear how, and why, designs might be used in national security investigations or, more broadly, to achieve national security ends. Similarly to UK unregistered designs, schedule 1 of the Registered Designs Act 1949 (RDA) also makes provisions for Crown use. Here too, however, in those circumstances – presumably relatively few – in which it is necessary to infringe design rights for national security purposes, the provisions of the ISA 1994 offer clear advantages over those of the CDPA and RDA.

[78] The subsection refers also includes 'foreign defence purposes' and 'health service purposes' as 'services to the Crown': CDPA, s 240(2). Section 244 CDPA also provides a specific exception for use during emergencies which would not seem to be relevant to intelligence services' operations generally.

4. NATIONAL SECURITY AND THE PUBLIC INTEREST IN SUBSISTENCE AND ENFORCEMENT

In this final section, we consider briefly those other ways in which national security considerations might be given effect in intellectual property law, with reference not to special rules of justification for what would otherwise be infringing use, but to rules which permit the refusal to find that a property right exists to begin with (ie rules affecting subsistence) or the refusal to enforce intellectual property rights on grounds other than those discussed above. Here, the relevant rules are not of exclusive relevance to national security, but encompasses it via reference to the public interest generally.

a. The public interest defence in copyright

Assuming that a given act constitutes an infringement of copyright and therefore an interference with a property right, the question arises of whether there might exist in law – beyond the statutory authority which the 1994 Act seems able to provide – a way for the alleged infringer to avoid liability. One possibility is that agents of the state engaging in activities constituting a prima facie copyright infringement could seek to take advantage of section 171(3) CDPA, which provides that '[n]othing in this Part affects any rule of law preventing or restricting the enforcement of copyright, on grounds of public interest or otherwise.'[79] This point was not raised in *Privacy International* but is worth considering in the context of the broader national security issues raised not only by hacking but by intelligence services' and other government work that (potentially) interferes with intellectual property. The key question here is whether the formulation of section 171(3) CDPA implies that such rules necessarily exist (and so creates them if they do not already do so), or instead only preserves those rules if they contingently exist independently of it.[80] Indeed, section 171(3) CDPA came into force after the common law had already recognised a public interest defence to infringement.[81] Whatever the current status of the public interest as a defence or ground for refusal to enforce copyright in the (allegedly) infringed work, section 5 ISA 1994 provides a potentially much broader avenue for the effective authorisation of interferences with copyright as property with respect to the security services. In its absence, a consideration of the public interest may lead the court to either refuse to enforce

[79] Note also the existence of a public order power in Article 17 Berne Convention but this – although referring to national security interests – seems to relate to censorship rather than interference with copyright. See also Ricketson, Sam, *WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment*, *Standing Committee On Copyright And Related Rights,* Ninth Session, Geneva, June 23 to 27, 2003, 2003, 75.

[80] On the nature of the public interest defence see J Griffiths, 'Pre-Empting Conflict - a Re-Examination of the Public Interest Defence in UK Copyright Law' (2014) 34 LS 1–27.

[81] In *Lion Laboratories v Evans* [1985] QB 526: Griffiths, 'Pre-empting Conflict', 5.

the copyright in a relevant work because the work itself is wrongful, *or* to find a defence to infringement exists because, in particular, a disclosure of the work was in the public interest.

In the case of a prima facie infringement of copyright not explicitly sanctioned by a specific statute such as the ISA 1994, a court may nevertheless excuse that act by, for example, refusing to enforce copyright because to do so would be 'injurious to public life, public health and safety…':.[82] With respect to the refusal to enforce, dicta in *Spycatcher*, for example, suggest that the conduct of a work's author (in this case breaching the Official Secrets Act in publishing an autobiography) might be considered 'disgraceful', such that the court for that reason declines to find that copyright subsists in the relevant work.[83] Any such judicial approach would be of particular interest to agents of law enforcement other than the security services, whose specific statutory powers of property interference are either far more limited than those of MI5, MI6 and GCHQ, or do not exist. Seeing that a restriction – on national security grounds – on the enforcement of intellectual property rights is contemplated in the Infosoc Directive (as discussed above), it is also possible to argue that even if a public interest defence falls outwith the defences contemplated by Article 5[84] that it may instead be covered by Article 9 Infosoc Directive.[85]

However, if the works being interfered with through hacking are not in and of themselves wrongful it will be necessary to ask whether any disclosure was in the public interest. That fact would potentially be relevant here, because, as the Court of Appeal found in *Ashdown*, disclosure of a copyright protected work which is necessary for a public interest purpose may activate the public interest defence.[86] To the extent that the security services may be disclosing evidence of wrongdoing – of a kind contemplated in *Lion Laboratories v Evans*[87] – the public interest defence is likely to succeed. And as Griffiths notes in this regard, '[t]he [public interest] defence has not traditionally been restricted to the functions of promoting public security or reporting current events.'[88] Yet it would seem that hacking is likely to lead to the copying and disclosure of material of a kind that is not in and of itself 'wrongful', and to that extent there are no clear parallels with *Lion Laboratories* available. That is, we are concerned here not with the conduct of

[82] *Hyde Park Residence Ltd v Yelland* [2001] Ch 143, [66].
[83] *Attorney General v Observer* [1990] 1 AC 109, 275-6 (Lord Griffiths).
[84] Arguing that an unalloyed defence of public interest may be inconsistent with the Infosoc Directive in light of the three-step test, but that would likely not be the case with respect to a national security justification: S Ricketson, *WIPO Study on Limitations and Exceptions of Copyright and Related Rights in the Digital Environment*, *Standing Committee On Copyright And Related Rights,* Ninth Session, Geneva, June 23 to 27, 2003, 2003, 75.
[85] Argument of Burrell and Coleman discussed in Griffiths, 'Pre_empting Conflict', 10. Article 9 reads 'This Directive shall be without prejudice to provisions containing in particular patent rights, trade marks, design rights, utility models, … trade secrets, *security*, confidentiality, data protection and privacy...' (emphasis added).
[86] See *Ashdown v Telegraph Group* [2002] Ch 157.
[87] [1985] QB 526.
[88] Griffiths, 'Pre_empting Conflict', 10.

the copyright owner, but solely with the motivation of the (alleged) infringer. We are left then with Mance LJ's observation in *Hyde Park v Yelland* that the application of the public interest defence cannot be precisely categorised.[89] Indeed, Phillips MR in *Ashdown* rejects the narrow view of Aldous LJ in *Hyde Park v Yelland* with respect to the scope of the public interest defence, preferring Mance LJ's position on this point.[90] We would argue that the infringement of copyright on national security grounds, especially given that the meaning of the public interest remains broadly undefined, may present a persuasive reason for making out a public interest defence despite not fitting neatly into existing categories covered in the case law and despite the fact that in a hypothetical case, the infringement would not take place in the context of a disclosure to the public (to which the present case law mostly relates).[91]

b. The public interest in patent and design law

Patent law does not operate a public interest defence as such but, in respect of the rules regulating patentable subject matter, the public interest (broadly conceived) is – in the 'public policy and morality' exception to patentability – a crucial element in determining whether property rights in the form of a patent will be granted over a particular invention.[92] The question for us is whether the protection of national security presents itself as a relevant consideration at the examination stage. The case law regarding public policy and morality (or, *ordre public* and morality) has tended to focus on the patentability of biotechnological inventions.[93] At the European level, the European Patent Office approach to patentable subject matter does reflect concerns with security. The EPO Technical Board of Appeal considers Art 53(a) and public security in *Plant Genetic Systems*,[94] saying 'It is generally accepted that the concept of 'ordre public' covers the protection of public security and the physical integrity of individuals as part of society'.[95] The EPO Guidelines refer to the kind of inventions falling under that heading as those: 'likely to induce riot or public disorder, or to lead to criminal or other generally offensive behavior… Anti-personnel mines are an obvious example.'[96] With respect to the kind of matters under discussion in *Privacy International*, it remains to be seen if a cybersecurity-related product or process would be considered the kind of invention that, due to its capacity to create public disorder, would be denied patent protection. This would, however, have to be a very particular

[89] *Hyde Park v Yelland*, [82].
[90] *Ashdown*, [58].
[91] ie adopting Mance LJ approach to publication that focuses not on the nature of the work but rather whether publication was significant 'in the context of other facts': *Hyde Park v Yelland* (n X) [82].
[92] PA 1977, s 1(3). Equivalent EPC art. 53(a) – *ordre public* and morality.
[93] See generally L Bently and B Sherman, *Intellectual Property Law* (OUP 2014), 519-20.
[94] *Plant Genetic Systems/Glutamine Synthetase Inhibitors v (Opposition by Greenpeace)* [1995] EPOR 357.
[95] *Ibid*, 366.
[96] *EPO Guidelines* Part G, Chapter II, 4.1. See also Bently and Sherman, *Intellectual Property Law*, 519-20.

case given the plethora of benign technologies that might be used for less than benign ends. A similar hurdle in terms of providing intellectual property right protection may be found in the law relating to registered designs. Section 1D RDA provides that '[a] right in a registered design shall not subsist in a design which is contrary to public policy or to accepted principles of morality.'[97] The relevant RDA schedule also identifies specific categories that will be excluded and does not provide for a national security or similar exemption for the registration of designs being concerned instead with the protection of, primarily, flags and emblems.[98] Nevertheless, as with certain inventions, we might imagine that an attempt to register a design that would be prejudicial to national security would be unsuccessful.[99] Regarding the UK unregistered design right in the CDPA, there is no specific national security exception but there is a public interest provision in section 238 regarding the exercise of certain powers.[100] That such rules might be employed for the converse purpose of refusing a patent to some invention which may be beneficial to security – rather than refusing it because it is harmful thereto – seems unlikely, but that question is of course less urgent in the context of those provisions, described above, which make it possible for the Crown to interfere with property, or to use (or authorise others to use) such inventions or designs. Better from a pragmatic point of view to recognise the patent and then make Crown use of it – without notice, if the public interest demands it.

Even where intellectual property rights are recognised, considerations of national security may see those rights treated differently within the relevant legal framework. The publication rules in the PA 1977 explicitly consider matters of national security with allowing for the publication of information that is 'prejudicial to national security'[101] to be restricted under certain conditions. Moreover, where such restrictions are in force a patent will not be granted.[102] Indeed, as the IPO itself points out, every patent application is screened 'to identify any which could be prejudicial to national security or public safety'.[103] IPO guidance is provided on the types of inventions that may be viewed as sensitive in terms of national security – for example relating to atomic energy,

[97] The equivalent Directive 98/71 on the legal protection of designs OJ L 289, 28-35 exclusion is found in Article 8. But note recital 16 stating that 'this Directive does not constitute a harmonisation of national concepts of public policy or accepted principles of morality'.
[98] See also restrictions regarding registration: Trade Marks Act 1994, s 4 (protected emblems) and s 3(3)(a) (public policy and morality).
[99] Of course, such a refusal does not prevent the creation, or marketing etc of a problematic design. To that extent, intellectual property law is severely limited in its usefulness as a tool to enhance national security.
[100] Including under Competition Act 1980, s 12.
[101] The section refers also to public safety. Note that the EPC does not have a similar provision relating to national security.
[102] PA 1977, s 22(3)(a).
[103] Intellectual Property Office, 'National security checks on patent applications' 9 May 2014, [https://www.gov.uk/guidance/national-security-checks-on-patent-applications].

'[c]ipher, code, encryption, secrecy and privacy systems and devices'[104] – but the list is incomplete for being redacted, presumably also on national security grounds. The application itself is considered within the Security Section before being forwarded, if no issues arise, for general examination.[105] The decision to restrict the publication of the patent application cannot be appealed.[106] Similarly, section 5 RDA enables the publication of certain information relating to designs 'relevant for defence purposes' to remain secret. What we see in this overview of public interest concerns in the regulation of patents and designs in particular is that the capacity to take into account matters of national security is embedded in the regulation of intangible assets from technical matters of procedure to the recognition of subsistence and, finally, the availability of defences and damages when an infringement does occur.

5. CONCLUSION

Through the public interest defence, Crown use provisions, and rules relating to subsistence amongst others, the existing intellectual property regime offers a number of mechanisms which may effectively legitimate interference with intellectual property for national security ends. The judgment of the IPT, however, confirms that in the specific context of the work of the security services, there exist powers which – in their breadth and their secrecy – are of potentially far more significance, and which apply not just to copyright (as was the focus of the IPT's judgment) but, we have suggested, to all intellectual property rights. Warrants granted under section 5 ISA 1994 enable the security services to interference with intellectual property rights in a manner that is both general and highly flexible, not requiring them fit within existing subsistence and compulsory licensing rules (as relevant) nor exposed to the uncertainties inherent in providing an after-the-fact defence to the infringement of intellectual property rights. The matters relating to copyright raised in *Privacy International* are, given that judgments of the IPT can be neither appealed[107] nor – the relevant statute suggests – judicially reviewed,[108] likely to be the source of on-going political and legal contention. The means of interference with intellectual property at the disposal of the state (as with those of interference with property

---

[104] Intellectual Property Office, *Technology which may be subject to section 22 of the Patents Act 2004*, [https://www.gov.uk/government/publications/technology-prejudicial-to-national-security-or-public-safety] 4.
[105] Intellectual Property Office, *Manual of Patent Practice*, version published July 2016 at [22.03].
[106] PA 1977, s 97(1)(c). The decisions in question are those made under PA 1977, s 22(1) and (2).
[107] Regulation of Investigatory Powers Act 2000, s 67(8), providing that '[e]xcept to such extent as the Secretary of State may by order otherwise provide, determinations, awards, orders and other decisions of the Tribunal (including decisions as to whether they have jurisdiction) shall not be subject to appeal…'. No orders have been made to permit such an appeal.
[108] Regulation of Investigatory Powers Act 2000, s 67(8). Notwithstanding that provision, Privacy International has indicated an intention to seek judicial review of the IPT decision: [https://www.privacyinternational.org/node/862]. See also Statement of Facts and Grounds, 6 May 2016 especially regarding copyright (at [12] and [22]) and the effect of the RIPA ouster clause (at [50]-[57]): [https://privacyinternational.org/sites/default/files/Grounds_1.pdf].

generally), will change again with the enactment of what is currently the Investigatory Powers Bill, which sets out the framework for new powers of 'equipment interference'[109] (the new and preferred terminology for what was previously described as CNE) which are both more intrusive and subject to greater safeguards than are those contained in the 1994 Act. Those powers will, however, be left intact and in fact extended by the Bill as it currently stands, which amends the ISA so as to permit property interference by MI6 and GCHQ in the British Islands even for the purpose of preventing and detecting 'serious crime'.[110] Given the discussion in this article, this represents also an important, and largely unaddressed, extension of powers of interference with intellectual property.

[109] Investigatory Powers HL Bill (2015-16, 2016-17) 56/2, Part 5 and Part 6, Chapter 3.
[110] *Ibid*, cl 227(3).