ASSANGE, WIKILEAKS, AND THE LIABILITY OF WIKI PROVIDERS FOR THIRD PARTY CONTENT

by **Richard I. Copp***

* *Business Law Group, Griffith Business School, Griffith University, Nathan, Brisbane Australia*

Abstract

The uploading of U.S. diplomatic cables onto the WikiLeaks' wiki website has sparked outrage in the United States, Australia and the United Kingdom. After more than a year, U.S. authorities are reportedly still considering whether they can prosecute WikiLeaks and its founder Julian Assange. This paper investigates the grounds under U.S. and Australian Federal law for prosecuting both, and the implications of the case for information technology (IT) law. Conviction under U.S. law would most likely be based on unlawful receipt or unauthorised possession of information which could injure U.S. interests; failing to remove offending material from the wiki within a reasonable time; and "aiding" the uploading of the stolen material albeit passively, by providing a wiki on which they could be anonymously posted by a third party. Given the reported evidence, there are no serious grounds for prosecution under Australian Federal law. Nonetheless, the analysis has important implications for IT law. Wiki providers – and so-called 'mirror' websites – would appear not to be liable for publishing on their wikis for defamatoroy or other material that does not clearly threaten national security, since they do not 'publish' material but merely make available a conduit for others to publish it. Nevertheless, a prudent wiki provider would monitor site content and remove very sensitive information. Finally, if self-regulation by wiki providers cannot prevent community harm or risks to national security, there may be grounds for internationally regulating wikis and mirror sites.

1. Introduction

There has been vociferous debate and even outrage over WikiLeaks' reported decision in early 2010 not to remove from its cache more than 250,000 U.S. diplomatic cables dating from the 1960s through to February 2010 (MacAskill 2010; Benkler 2011, p. 313). Reportedly, only about 280 of these cables can be accessed direct from WikiLeaks.org itself, although access to all of the cables was permitted for *Der Spiegel*, *Le Monde*, *El País*, and *The Guardian* (UK) newspaper, who apparently released them to *The New York Times* (Adams 2010; Benkler 2011, p. 312). Much of the media scandal was due to the fact that official reports of the Allied forces' conduct and operational effectiveness in the Afghanistan and Iraq wars was directly contradicted by some of this leaked material. The leaks included a 39-minute U.S. military video showing a helicopter airstrike that resulted 12 civilian deaths, including those of two Reuters journalists (Green 2012, p. 97).

While WikiLeaks has never confirmed who uploaded the cables to its wiki in the first place, the source was reportedly a U.S. Army intelligence analyst, one Private First Class (Pfc.) Bradley Manning who, while serving in Iraq, allegedly downloaded them from the Secret Internet Protocol Router Network (SIPRnet). This is a system of information technology (IT) networks used by the U.S. Defense and State Departments to pass 'classified' information between the U.S. and selected allies such as the UK and Australia. Manning was arrested in May 2010 and, after confessing, is now incarcerated in a military prison in Virginia awaiting trial.

In the wake of these events, WikiLeaks reportedly lost the support of a number of its major corporate sponsors who apparently provided it with much-needed funding. For example, Amazon.com decided to no longer host WikiLeaks resources on its servers; PayPal refused to process credit card donations and payments relating to WikiLeaks' activities; Apple elected to withdraw a WikiLeaks App from its Apps store; and a number of credit card and payment companies including MasterCard, Visa, and Bank of America cut off the ability of people and companies to donate to WikiLeaks using their payment services (Brunton, 2011, p. 19; Benkler 2011, pp. 314, 339-342; MacAskill 2010; Haynes 2010).

Julian Assange is no doubt a controversial figure, whose notoriety is fuelled by his prior convictions for computer hacking (Lagan 2010); allegations of sexual misconduct in Sweden (Davies 2010; Leigh et al 2010; Rundle 2010); and possibly statements he allegedly made in private, rather than publicly, in the United States (Traynor 2010). Nevertheless, while he may well until recently have been the 'front man' for, and high profile face of WikiLeaks, Julian Assange is not WikiLeaks. Whatever Assange may or may not have done, there are broader issues at stake that potentially impact on many more people than just one individual. Self-evidently, allegations of sexual offences against Assange have nothing to do with the implications of the WikiLeaks model for IT law.

After more than a year, U.S. authorities are reportedly still considering options for prosecuting Assange - and presumably WikiLeaks (Dorling 2012). Accordingly, the purpose of this paper is to examine whether a wiki provider such as WikiLeaks could, with its personnel, be liable for any breaches of U.S. or Australian Federal law; and to identify some of the broader legal implications of the case for wiki providers and IT law generally. The paper fills a gap in the current literature in these respects, but also by clarifying the nature of a wiki, and questioning whether wiki providers can be penalised in law for 'publishing' any of the content uploaded by others to their sites.

The paper focuses only on those U.S. and Australian Federal statutory provisions that are capable, as a matter of construction, of applying to WikiLeaks' or Assange's conduct. It intentionally eschews discussion of the economic incentives or ethics underlying the WikiLeaks phenomenon; whether diplomatic and defence information is subject to 'over-classification' (in the sense of 'classified' information)[1]; and any discussion of UK extradition law or Assange's liability under Swedish criminal law for alleged sex crimes.[2] The literature and media reports are already replete with contributions relevant to all these aspects of the debate.[3]

The structure of this paper is as follows. Section 2 explains the concept of a wiki, while section 3 sets out the legal arguments concerning whether WikiLeaks or Assange have committed crimes under U.S. and Australian Federal law. Finally, section 4 identifies some of the key practical implications of the case.

2. The Nature of a Wiki

The word 'wiki' is derived from the Hawaiian for "quick" (Bean and Hott, 2005). The Oxford Dictionary (2010) defines a wiki is "*a website or database developed collaboratively by a community of users, allowing any user to add and edit content*." In short, a wiki is a real-time editable Web site whose content is iteratively created through users' cooperative efforts. It differs from a blog in that a wiki permits the uploading of content by multiple providers, whereas the content of a blog is provided by only one person – the blogger (Leuf and Cunningham, 2001; Bean and Hott, 2005; Hasan and Pfaff 2006). A so-called 'mirror site' is "*a copy of the contents of a network site at another site, typically in order to improve accessibility*" (Oxford 2010; Brunton, 2011, p. 19). A so-called '*live mirror*' updates automatically as soon as the original is changed.

Although wikis typically enable web content to be authored collectively, that web content is not redacted by any editorial process prior to its uploading or publication (Wagner 2004, p. 269). Many wiki providers invite users to themselves edit any page or to create new pages within the website. Because of this, the wiki provider simply provides a conduit by which a user who wishes to upload content can publish or disseminate it.[4] It must also follow that, to argue a wiki provider should 'vet' sensitive or dangerous information before it is uploaded by a user, or be legally culpable for failing to 'vet' such information before it is uploaded by a user, would be a category error in logic. For, if the provider did this, it would by definition not be providing a wiki.

In the case of WikiLeaks, whistleblowers who posted information on the WikiLeaks website were guaranteed that they would remain anonymous (Benkler 2011, p. 320). Since late 2010, however, a key problem for Wikileaks has been that the programming expertise behind

---

1 *United States v Rosen* 445 F Supp 2d 602, 633 (E.D. Va. 2006) per Judge Ellis; and Papandrea (2007, p. 278).

2 At the time of writing, Assange is under house arrest in the UK, awaiting a U.K. Supreme Court decision on whether he will be extradited to Sweden for alleged sex crimes.

3 Among others, see Macey (2007), De Poorter and Mot (2006), Moore (2011), Hasan and Pfaff (2006), Adley (2011) and Robinson (2012).

4 In some respects newspapers and other journalistic media are analogous, except that – traditionally at least – journalistic media has tended to be associated with redaction of content at some stage of the process, rather than simply providing a conduit for the material to be read in its original (unedited) form.

WikiLeaks' guarantee of anonymity for whistleblowers – a programmer euphemistically and somewhat melodramatically known in media circles as 'The Architect' – reportedly departed the organisation at about that time after a falling out with Assange. The Architect reportedly absconded with the computer code that guaranteed third party anonymity when submitting leaked information. According to former WikiLeaks deputy, Daniel Domscheit-Berg, Assange had no role in creating the anonymous submission system, nor any access to it (Fowler 2011a, 2011b; Domscheit-Berg 2011, pp.122-127, 228). Since 'the Architect's' alleged departure, Wikileaks has reportedly been unable to accept online submissions. If true, 'the Architect's' departure is likely to have been at least as damaging for WikiLeaks' continuing operations as any withdrawal of funding or funds payment platforms such as PayPal.

3. Legal Arguments

Plainly Pfc. Bradley Manning, who has himself confessed to releasing classified information to WikiLeaks, could be prosecuted under a myriad of U.S. laws, including (in declining order of seriousness):

1) 'Aiding the Enemy' under §904 Art. 104(2), on the basis that he knew (or ought reasonably to have known) that the intelligence - ie. classified documents - he posted without authority on the WikiLeaks website could indirectly be communicated to the enemy. Conviction would carry the death penalty, although this would likely be commuted to life imprisonment;

2) §793(e) of the *Espionage Act* 1917 [18 USC §793(e)] – for unauthorised access to, and communication of, documents relating to U.S. national defence to any person (eg. WikiLeaks) not entitled to receive them;

3) 18 USC §952 (2006), which prohibits the unauthorised disclosure of official diplomatic correspondence - eg. diplomatic cables - by U.S. Government employees;

4) §1030(a)(1) of the *Computer Fraud and Abuse Act* (CFAA) Supp. III 2010 – for knowingly or intentionally accessing classified files without authorisation and then using that information in an unauthorised way (eg. by wilfully transmitting the information to an unauthorised person – WikiLeaks) while having reason to believe that the information could be "used to the injury of the United States").

   The maximum penalty for conviction under these last three offences would be 10 years' imprisonment in each case[5] ; and

5) wrongful disposition of U.S. military property under §908 Art. 108(1) and (3), on the basis that, without authority, he either wilfully or otherwise disposed of U.S. military property, being diplomatic cables. If convicted, Pfc. Manning would presumably be court-martialled.

According to Benkler (2011, p. 338), Manning is most likely to be prosecuted for contraventions of the *Computer Fraud and Abuse Act*, although others (eg. Cloud 2011; Fadel 2010) have noted the potential for other more serious charges under U.S. law. Pfc.

[5] Cf. 18 USC §1924.

Bradley Manning is crucial to any prosecution case against WikiLeaks or Assange since, upon being exposed, he confessed to posting the offending U.S. diplomatic cables. Yet Pfc. Manning has never implicated Assange or anyone else at WikiLeaks in any conspiracy. Plainly, if he were to do so, the task of U.S. prosecuting authorities would be made a great deal easier.

Obvious questions arise about whether WikiLeaks or Assange could be indicted under U.S. or Australian Federal law, irrespective of Manning's testimony; and about the important broader implications for other wiki providers and IT law generally.

U.S. Law

Much of U.S. anti-terrorism law is clunky, anachronistic, and unsophisticated – based on assumptions that terrorist acts encompass planes flying into a building, suicide bombs by Al Qaeda, the manufacture of weapons of mass destruction, or possibly biological warfare. It is ill suited to prosecuting non-citizens for providing a wiki via which the public can peruse embarrassing classified government information. In the absence of testimony from Pfc. Manning, any prosecution case against WikiLeaks or Assange[6] appears to turn upon whether:

(1) a wiki provider could be criminally liable for the passively receiving or possessing illegally obtained information, as distinct from actively publishing, disclosing or otherwise using the information to its advantage; and whether the First Amendment to the U.S. Constitution protects freedom of speech when U.S. national security is threatened;

(2) they had the requisite purpose or intent – eg. to "purposefully and materially support hostilities", or 'intentionally endanger U.S. national security";

(3) they had constructive knowledge – eg. that their activities could aid the enemy, or endanger U.S. interests;

(4) whether there is sufficient circumstantial evidence to convict for conspiracy or 'party' offences; and

(5) they could be charged with U.S. or Australian crimes enacted pursuant to mutual treaty obligations.

Each issue will be examined *seriatim*.

(1) Receipt and Possession vs. Disclosure, Use, Publishing and the First Amendment

There is little doubt that the information forwarded to WikiLeaks by Manning was property of the U.S. Government, and that WikiLeaks personnel would have known this upon perusal of it. Benkler (2011, p. 364) has argued that "*passive receipt of illegally obtained materials is...not subject to prosecution*", reasoning that if prosecution under this head were likely to successful, then the journalists in the *Pentagon Papers* case[7] and *Bartnicki v Vopper*[8] who

[6] Nonetheless, national security and defence-related criminal law, which applies extra-territorially if there is a sufficient nexus with the home jurisdiction (Neuman 1991; Cabranes 2009), would appear to be most relevant body of Federal law for prosecutorial purposes.

[7] *New York Times v United States* 403 US 713 (1971).

received material from someone who themselves had contravened criminal law in forwarding the materials, would have been liable. However, this is oversimplistic. A distinction must be drawn between passive receipt or possession, and actively dealing with the information.

With regard to passive receipt or possession, U.S. authorities could prosecute WikiLeaks, and possibly Assange, for:

- "unlawful receipt" of national defence documents, knowing or having reason to believe they were obtained illegally: 18 USC §793(c);

- "unauthorised possession" of national defence documents which, having reason to believe they could be used to injure the U.S. or advantage any foreign nation, are wilfully retained and not returned to the U.S. Government: 18 USC §793(e). Given the wording of this section, a wiki provider could even be criminally liable for failing to remove sensitive or dangerous information from its wiki as quickly as is practicable, or at least within a reasonable time; and/or

- "receiving" or retaining anything of value belonging to the United States or any its Departments or agencies, knowing it to have been stolen, with intent to convert it to their own use: 18 USC §641. Conviction carries a maximum term of ten years' imprisonment.

Whether WikiLeaks or Assange could be convicted under these provisions would depend on whether the evidence satisfies the other key elements in those sections, as discussed below. However, to the extent that these provisions penalise passive receipt or possession of illegally obtained material, Benkler (2011, p. 364) is wrong to claim that "*passive receipt of illegally obtained materials is...not subject to prosecution".*

The situation is different for an accused that actively discloses, uses to their advantage, communicates or publishes illegally obtained material. Relevant U.S. law in this context includes the following:

- intentional "disclosure" of electronic communications to unauthorised persons, knowing or having reason to know that the information was obtained illegally by electronic means. Conviction renders offenders liable to imprisonment for up to five years: 18 USC §2511(1),(3)(a), (4)(a);

- unauthorised "disclosure" of the identities of U.S. undercover intelligence officers: 50 USC §421(a),(b) or (c);

- "use" of classified information in a manner prejudicial to U.S. interests or to the benefit of a foreign government, conviction for which carries a term of up to 10 years' imprisonment: 18 USC §798(a); and/or

- "communication" (or causing to be communicated) to any unauthorised person illegally obtained national defence documents where there is reason to believe they could be used to injure the U.S. or advantage any foreign nation: 18 USC §793(e).; and/or

---

[8] 632 U.S. 514, 528 (2001).

- Publishing sensitive material illegally obtained.

The Oxford Dictionary (2010) defines each term as follows. To "*disclose*" is to "*make secret or new information known*". The noun "*use*" is defined as "*the action of using something*", while the verb "*use*" means "*to take, hold, deploy (something) as a means of accomplishing or achieving something*". To "*communicate*" is to "*share or exchange information*", while to "*publish*" as to "*communicate to a third party*". The choice of the language in each set of provisions is viewed by some as significant, since U.S. legislation sometimes uses one term but not the others. Some judges believe this to be deliberate on the part of the legislature[9], and it is crucial in the WikiLeaks case.

All of these terms imply affirmative action, rather than passive receipt. Accordingly, it is difficult to see how WikiLeaks could be in breach of any of the foregoing provisions. Being a wiki provider, WikiLeaks never (actively) disclosed, used, communicated or published anything, but merely provided the means for others (eg. Pfc. Manning) to do so.[10] This is the same reasoning why the owners of websites are generally not liable under U.S. law for offensive material posted on their sites by third parties whose identity cannot be determined.[11]

This distinction cuts across and clarifies much of the U.S. literature on the WikiLeaks case, which has assumed without question that a wiki provider actually 'publishes' or 'discloses' the material uploaded by others onto its site (eg. Papandrea 2007, Jones and Ward Brown 2011). It also cuts across much of that literature's distinction between whether the U.S. Supreme Court would impose an ex post, rather than a prior restraint on such a wiki provider (eg. Silver 2008; Benkler 2011; Stone 2004, 2011).

Even if this reasoning is wrong there may, depending on the circumstances, be some protection for wiki providers afforded by the First Amendment to the U.S. Constitution. The First Amendment, which applies abroad[12] even to non-citizens[13] accused of breaching U.S. laws, prohibits any law which abridges freedom of speech or infringes on the freedom of the press. For the sake of clarity, assume that "X" (eg. Manning) illegally obtains information and discloses or publishes it to "Y" (a wiki provider), who then discloses or publishes it to a third party "Z" when "Z" reads it on "Y's" wiki. Whether liability attaches to "Y" (the wiki provider) in U.S. law depends on whether the First Amendment protects "Y" from liability.

Based on the few U.S. Supreme Court decisions on record, if the intention of Federal legislation is to impose *civil* (not criminal) liability on "Y" for publishing the information, and:

---

9 See eg. *New York Times v United States* 403 US 713, 721-722 (Douglas J. concurring). But cf. *United States v Progressive* 467 F Supp 990, 995 (W.D. Wisc. 1979). See also Silver (2008, p. 473) and Elsea (2011, p. 13n) for opposing views on this point.

10 WikiLeaks did reportedly engage in minimal redaction of the U.S. diplomatic cables in its possession by deleting the names of U.S. undercover intelligence officers and operatives – but this was almost certainly acting responsibly because of the risk to these personnel, and not to do with the technical meaning of the word "disclosure" in 50 USC §421(a),(b) or (c).

11 47 USC § 230 (s. 230 of *Communications Decency Act* 1996). Inexplicably Federal criminal law is exempted: 47 U.S.C. § 230(e)(1) – but this was largely to minimise political opposition to the legislation.

12 *Downes v Bidwell* 182 US 244, 282-283 (1901).

13 *Yick Wo v Hopkins* 118 US 356, 374 (1886); *Boudemiene v Bush* 733 US 553 (2008).

(a) If punishing "Y" would probably *not* eliminate the market for "X's" (and others' similar) illegal activities, then the First Amendment right to publish truthful information on matters of public concern trumps any right of confidentiality, and "Y" cannot be legally restrained from publishing the information: *Bartnicki v Vopper*.[14] The initial wrongdoer "X" can, of course, be prosecuted for illegally obtaining the information in the first place. Alternatively:

(b) If punishing "Y" would probably eliminate the market for "X's" (and others' similar) illegal activities, then the First Amendment right to publish truthful information on matters of public concern is subservient to a right to confidentiality, and "Y" can be legally restrained from publishing the information: *Bartnicki v Vopper*. In addition, "X" can be prosecuted for illegally obtaining the information in the first place.

In contrast, if the intention of the Federal legislation is to impose *criminal* (not merely civil) liability on "Y" for receiving and publishing the information - as (say) the U.S. *Espionage Act* does[15] - and the U.S. Government seeks to restrain "Y" from actively publishing the information to "Z", but the Government:

(a) cannot establish that publication would result in a "*clear and present danger*"[16] to U.S. national security, then "Y's" publication of information to "Z" is protected by the First Amendment and "Y" cannot be legally restrained from publishing the information.[17] ("Y" may however, be convicted for publishing): *New York Times v United States*.[18] Alternatively:

(b) can establish a "*clear and present danger*" to U.S. national security, then the Government could presumably enjoin publication by "Y", who would not have First Amendment protection: *New York Times v United States*.

The latter proposition (b) makes intuitive sense. If "Y" knows that information was obtained illegally and that its publication would constitute a "clear and present danger" to U.S. national security, but nevertheless passes it onto "Z" (particularly if "Y" knows or ought to know that "Z" would pass it on to terrorists), then "Y" is effectively by its omission criminally negligent, and should be culpable.

There is another possible avenue for protection for some wiki providers afforded by the First Amendment – freedom of the press. As noted, the First Amendment prohibits any law that abridges freedom of speech, or infringes on the freedom of the press.

As a matter of statutory construction, the two limbs are plainly independent, so that strictly speaking there is no need for WikiLeaks or Assange to prove they are journalists to be afforded protection. Nonetheless, WikiLeaks and Assange plainly have an incentive not to discourage any characterisation of their work as journalistic. For example, WikiLeaks was recently awarded the prestigious Walkley Award in Australia for most outstanding contribution to journalism (Robinson 2012). Such independent professional peer recognition

---

14 632 U.S. 514 (2001).
15 18 U.S.C. § 793(c).
16 *Schenck v. United States*, 249 U.S. 47 (1919), per Justice Holmes.
17 403 US 713 at eg. 729-730 (1971). See also *Smith v Daily Mail Publishing. Co*. 443 U.S. 97, 103 (1979). *Bartnicki v Vopper* 632 U.S. 514, 528 (2001).
18 403 US 713 (1971).

by 'traditional' journalists would presumably figure prominently in a court's decision about whether WikiLeaks, and possibly Assange[19], are journalists entitled to First Amendment protection under the "free press" limb.

(2) Intent and Purpose

Some of the potential charges against WikiLeaks or Assange contain "intent" as a necessary element. These include:

- "intentional" disclosure of electronic communications to unauthorised persons: 18 USC §2511(1),(3)(a), (4)(a);

- "intentional" disclosure of information that could be used to discover the identities of U.S. undercover intelligence officers: 50 USC §421(a),(b) or (c)[20]; and

- "intent" to "injure the United States" or "advantage a foreign nation": 18 USC 794, and 18 USC 798A.

The Oxford Dictionary (2010) defines "*intent*" as "*the object to which the mind is directed*"; in law, it denotes the actual state of mind of an accused, which can be inferred from circumstantial evidence. Whether such inferences can be drawn, in the absence of evidence from witnesses such as Manning or perhaps others in the U.S. or elsewhere with whom Assange or others such as Domscheit-Berg have had contact, is a matter for the Court's discretion. However, insofar as any "intention" is directed only to "disclosure" in 18 USC §2511 and 50 USC §421, it is intention directed at affirmative action rather than passive receipt. WikiLeaks as a wiki provider never intentionally disclosed anything; rather it provided the means for others to do so.

In addition, there is no evidence on the public record to suggest that WikiLeaks or Assange "intended" to injure the U.S. or advantage a foreign nation.

Similarly, there is no evidence that WikiLeaks or Assange "purposefully" supported hostilities against the United States or its coalition partners", which is prerequisite to either being declared "unprivileged enemy belligerents".[21] An 'unprivileged enemy belligerent' is a civilian directly engaged in armed conflict in violation of the international laws of war, and may lawfully be detained or prosecuted under the domestic law of a detaining state.[22] Again according to the Oxford Dictionary (2010), "*purpose*" is "*the reason for which something is done*". It is possible for a person to act with several purposes in mind, but in law the requisite purpose must be the substantial or operative one.

---

[19] Assange has reportedly been a member of the Media section of the Media, Entertainment and Arts Alliance (formerly the Australian Journalists Association), which is the Australian professional organisation for journalists. In 2011, he was made an honorary member.

[20] As noted, WikiLeaks reportedly engaged in minimal redaction of the U.S. diplomatic cables on its site by deleting the names of operatives.

[21] 10 USCA §948a(7), 10 USCA §950v(27).

[22] See the Third and Fourth Geneva Conventions on the Treatment of Prisoners of War (1929), and on the Protection of Civilian Persons in Time of War (1949), respectively.

If WikiLeaks and Assange did nothing but provide the means by which others could publish information, it is difficult to see that the *reason* for doing so was to support hostilities (as distinct from eg. enhancing transparency and public knowledge in a democratic setting). The case against Australian David Hicks would have been considerably stronger in this regard (Hicks, 2010). Thus, any declaration that WikiLeaks or Assange were "unprivileged enemy belligerents" would very likely be subject to successful legal challenge.

(3) Knowledge or Belief

Some relevant U.S. provisions require either an accused to have knowledge "or" reason to believe, that information received by them was illegally obtained in the first place, or that the information could be used to harm U.S. interests:

- "knowing" or "having reason to know" that information disclosed to unauthorised persons, was originally obtained illegally: 18 USC §2511(1),(3)(a), (4)(a);

- "knowing" or "having reason to believe" that defence documents unlawfully received were obtained illegally: 18 USC §793(c);

- "knowingly" communicating classified information in a manner prejudicial to U.S. interests or to the benefit of a foreign government: 18 USC §798(a); and

- "knowing" that information could be used to discover the identities of U.S. undercover intelligence officers, but nonetheless disclosing it without authorisation: 50 USC §421(a),(b) or (c).

Unless the relevant statute specifies 'actual knowledge', 'constructive' knowledge would normally be sufficient to satisfy the element of 'knowledge'.[23] That is, the element would be fulfilled if the prosecution could prove the recipient – eg. a WikiLeaks – knew or ought reasonably have known[24], beyond reasonable doubt, that information on its wiki was (respectively) obtained illegally; communicated in a manner prejudicial to U.S. interests; or a means of identifying covert U.S. operatives. Ironically, the fact that WikiLeaks' reported minimal redaction of the U.S. diplomatic cables in its possession by deleting the names of U.S. operatives suggests that WikiLeaks did know that the cables could be used to identify those operatives. Moreover, it stretches belief to suggest that WikiLeaks did not know, either actually or constructively, that material uploaded by Pfc. Manning was illegally obtained. It is therefore unlikely that WikiLeaks – or possibly Assange, depending on his involvement – could escape this mens rea aspect of these offences.

Whether they could be convicted under these provisions would, however, depend on whether the evidence satisfies the other key elements in those sections. As discussed earlier, based on the meanings of the elements 'disclosed' (in 18 USC §2511 and 50 USC §421), 'communicate' (in 18 USC §798(a)), this is unlikely. Having said that, it is possible that WikiLeaks and possibly Assange could be convicted of "knowing" or "having reason to believe" that defence documents unlawfully received were obtained illegally: 18 USC §793(c).

---

[23] Cf. Stern (2007).

[24] Cf. *United States v. Twiss* 127 F.3d 771, 774 (8th Cir. 1997)*; United States v. Bernard* 623 F.2d 551 (9th Cir. 1980). *; United States v. Wright* 641 F.2d 602 (8th Cir. 1981); and Stern (2007).

(4) Conspiracy/Party Offences

A key problem with charging WikiLeaks or any of its personnel with conspiracy-related offences is that any evidence of a common intent or unlawful purpose with Pfc. Manning would necessarily be circumstantial, and may well fail to reach the criminal threshold of "beyond reasonable doubt'".

This problem is likely to infect any U.S. Government prosecutions for:

- conspiring with Pfc. Manning to, without authorisation, communicate or cause to be communicated to a foreign person any information relating to U.S. national defence which would be used to injure the United States": 18 USC §793(g) of the *Espionage Act* 1917;

- conspiracy to gather or deliver defence information to aid a foreign government: 18 USC §794(c);

- seditious conspiracy, which has a maximum penalty of 20 years' imprisonment: 18 USC § 2384;

- conspiracy to commit a computer-related crime: 18 USC §1030(b); or

- conspiracy to commit any offence against the United States, which has a maximum penalty of 5 years' imprisonment: 18 USC §371

The prospects of a successful prosecution may, however, be enhanced if WikiLeaks or Assange could be said, in terms of 18 USC §2, to have "aided" Pfc. Manning's crimes, even if only by passively providing a wiki on which he could anonymously post the illegally obtained documents.

(5) Treaty Obligations between U.S. and Australia

Ironically, the U.S. and Australia have agreed to share their national security technology and information (Commonwealth of Australia 2010, p. 46), but this is precisely the technology and information that Pfc. Manning used to access the diplomatic cables whose posting on WikiLeaks caused such furore in the first place.

Both countries are signatories to a number of anti-terrorism treaties such as the International Conventions for the Suppression of Terrorist Bombings, the Financing of Terrorism, and Acts of Nuclear Terrorism (ATS 2002a, 2002b, 2002c); agreements to prevent nuclear proliferation and weapons of mass destruction (eg. Commonwealth of Australia, 2010, p. 52); and the Convention to punish 'acts of terrorism' including crimes against persons and extortion (United Nations, 1989).

Yet these are ill suited to prosecuting wiki providers whose sites include embarrassing classified information. Indeed, none of these international treaties or agreements, nor any of

the attendant legislation[25] (other than that discussed) criminalises the provision of a wiki onto which third party users can anonymously post sensitive or dangerous information.

Summary

Of the offences outlined, it is possible that WikiLeaks and possibly Assange could be convicted in the U.S. of:

- unlawful receipt of national defence documents, knowing or having reason to believe they were obtained illegally: 18 USC §793(c);

- unauthorised possession of national defence documents which, having reason to believe they could be used to injure the U.S. or advantage any foreign nation, are wilfully retained and not returned to the U.S. Government: 18 USC §793(e). Given the construction of this provision, WikiLeaks or Assange could also possibly be prosecuted for failing to remove the offending information from their wiki as quickly as is practicable, or at least within a reasonable time;

- receiving or retaining anything of value belonging to the United States or any of its Departments or agencies, knowing it to have been stolen, with intent to convert it to their own use: 18 USC §641. Conviction carries a maximum term of ten years' imprisonment; and

- "aiding" in crimes committed by Pfc. Manning, even if only by passively providing a wiki on which Manning could anonymously post the illegally obtained documents: 18 USC §2.

Australian Law

In many ways, relevant Australian law is similar to U.S. law. Constitutionally, the defence power extends to defence against terrorists acts committed within Australia[26]; and in any case, if there were a nexus with Australia, the Federal and High Courts would have extra-territorial jurisdiction.[27]

However, the Australian Federal Police in December 2010 announced that, in respect of the leaked U.S. cables, neither WikiLeaks nor Assange had committed any crime over which Australia had jurisdiction (Welch 2010). Moreover, two of the most qualified lawyers in the Australian Parliament, shadow Minister for Communications and Broadband Malcolm Turnbull, and shadow Attorney-General George Brandis SC have both reportedly emphasized that even 'publication' of classified material of foreign powers is not a crime in Australia (Robinson 2012).

---

[25] Treaties are given effect by the enactment of relevant legislation in each signatory's jurisdiction: *Koowarta v Bjelke-Petersen* (1982) 153 CLR 168; *Commonwealth v Tasmania* (the *Tasmanian Dams* Case) (1983) 158 CLR 1.

[26] *Thomas v Mowbray* (2007) 233 CLR 307; and s. 100.3 of the *Criminal Code Act* 1995 (Cth).

[27] See eg. Part 2.7, Div. 15 of the *Criminal Code Act* 1995 (Cth); and the *Terrorism (Commonwealth Powers) Acts* 2002, enacted in each of the States.

At first, this might seem somewhat surprising. Yet, because of the language of the relevant Australian provisions, both conclusions appear correct, as the following 'sample testing' of potential grounds for prosecution shows:

- 'Receiving stolen property' under s.132.1 of the *Criminal Code Act* 1995 (Cth) requires the accused to have *dishonestly* received the stolen property. There is no evidence that WikiLeaks or Assange did so;

- criminal negligence in failing to remove dangerous information from the wiki in a timely manner would require causal proof of Australian Defence Force (ADF) personnel deaths or injuries. Again, there is no such evidence, rendering ss. 5.5, 12.4 of the *Criminal Code* (Cth) nugatory;

- the same would apply to a charge of recklessly causing serious harm to an Australian citizen or a resident of Australia under s. 115.4 of the *Criminal Code* (Cth); reckless indifference causing injury or death to ADF personnel, under ss. 5.4, 5.6 of the *Criminal Code* (Cth); recklessly causing harm to United Nations Organisation or associated personnel, under s. 71.7; and intentionally causing harm to a U.N. or associated person, pursant to ss.71.6 and 5.2;

- "aiding" in crimes is an offence under s. 11.2(1) of the *Criminal Code* (Cth), but Pfc. Manning committed no crime under Australian Federal law – it therefore cannot be said that WikiLeaks or Assange 'aided' in a crime over which Australia has any jurisdiction;

- neither WikiLeaks nor Assange appear to have contravened s. 80.1 of the *Criminal Code (Cth)* in relation to treason, since there is no evidence they were waging war on Australia. Nor could they be convicted of intentionally assisting Australia's enemies under ss. 80.1AA and 5.2, since there is no evidence of the requisite intent;

- Similarly, there is no evidence of any intent to prejudice Australia's security, which is prerequisite to a charge of espionage or similar activities under ss. 91.1 and 5.2.

- While the U.S. cables could not have been accessed under Freedom of Information because that legislation exempts documents that are communicated confidentially by a foreign government[28], providing a wiki on which a third party can post them is not a crime under Australian Federal law;

- Charging WikiLeaks or Assange with possessing things connected with a 'terrorist act' under s.101.4 would probably be unsuccessful, because a particular 'terrorist act' could not be identified.[29] Similarly, there is no evidence of WikiLeaks or Assange supporting a designated 'terrorist organisation'[30]; and

- conspiracy to commit any of these crimes under s.11.5 of the *Criminal Code* (Cth) would presumably fail on the same evidentiary grounds in Australia as it would in the

---

28 *Freedom of Information Act* 1982 (Cth), s. 33.
29 *Lodhi v R* (2006) 199 FLR 303.
30 Section 102.1(2), (2A).

> United States. At most, it might be alleged that WikiLeaks members 'agreed' to cause a public mischief – but this does not constitute a conspiracy under Australian law.[31]

Similar problems would arise for any prosecutions under the *Australian Security Intelligence Organisation Act* 1979 (Cth), the *Cybercrime Act* 2001 (Cth), or the *Anti-Terrorism Acts No. 1* and *2* (Cth). There would appear, then, to be no evidence on which to base the laying of charges against WikiLeaks or Assange under Australian Federal law.[32]

4. Implications

We conclude that WikiLeaks and possibly Assange could be prosecuted and perhaps convicted of crimes under U.S., but not Australian, Federal law.

The WikiLeaks case is important, however, not only for its own sake and for that of clones such as OpenLeaks, BrusselsLeaks and Al Jazeera's Transparency Unit, but also because of its broader implications for IT law.

First, in both U.S. and Australian law, wiki providers and so-called 'mirror' websites would not be liable for 'publishing' sensitive government information on their sites since they do not 'publish' the material but merely make available a conduit for others to publish it. This has implications for defamation law as it affects wikis and mirror sites in both countries. Relevantly, the Supreme Court of Canada in 2011 held that someone who posts hyperlinks on a site which take the user to another site housing defamatory content, is not "publishing" defamatory material.[33]

Second, wiki providers need not therefore be ever 'on the lookout' or taking precautions to 'vet' sensitive information that might be placed on the wiki, since wikis by definition do not redact material that third parties upload. Nonetheless, it would be prudent and socially responsible of wiki providers and mirror sites to remove potentially dangerous information from their wikis as they become aware of it.

Third, while wiki providers with U.S.-based leaks may take some comfort from the fact that the U.S. Supreme Court has not yet convicted anyone other than a government employee for publicly disseminating such sensitive information (Stone 2011, p. 113), the risk of prosecution remains significant given the construction of some U.S. statutes (cf. also Silver 2008, p. 483).[34]

---

[31] *White v Director of Military Prosecutions* (2007) 231 CLR 570; *R v Boston* (1923) 33 CLR 386; 30 ALR 185; *Director of Public Prosecutions v Withers* [1975] AC 842.

[32] There is of course in Australia no equivalent of the First Amendment to the U.S. Constitution. Apart from this, the law on defamatory material being uploaded onto a wiki is conceptually similar. Rather than 'publishing' such material, a wiki provider simply provides a conduit for others to do so unredacted.

[33] *Crookes v. Newton* [2011] SCC 47; [2011] 3 SCR 269. Neither the U.S. Supreme Court nor the High Court of Australia has had reason to decide an analgous case. In Australia, the High Court has characterised defamatory material on a conventional website outside Australia as "published" in Australia when it was downloaded or read by someone in Australia, but that website was not a wiki: *Dow Jones & Company Inc v Gutnick* [2002] HCA 56.

[34] This may even affect merely inquisitive users. Benkler (2011, pp. 343, 350) highlights disturbing communications from U.S. University careers offices to their students, warning them not to read the WikiLeaks cables online because it could impair their prospects of employment with the U.S. government. (Curiously, students who read material on websites that "*the provider or user considers to be obscene, lewd,*

Fourth, while extant treaties to which the U.S. and Australia are signatories do not criminalise wiki providers and 'mirror' websites making their sites available as conduits for others to publish sensitive government information, it is possible in the aftermath of the WikiLeaks case that measures will be ratified in treaties over the next few years (cf. Opper 2011).

Fifth, whether a 25-year moratorium on releasing archived confidential Government material is still necessary in an age when new clone' wiki sites are increasingly emerging, is open to debate. Pragmatism suggests it is, provided future massive leaks are minimised. Certainly, document dumps involving one of the world's great powers are unlikely to recur, if only because IT security systems will now ensure that all access to confidential material is trackable (cf. Brunton 2011, p. 19).

Sixth, WikiLeaks itself may well become a martyr to the cause of transparency through technology. But the death of the WikiLeaks concept would be a pity. Leaks are by their nature embarrassing, but the real cause of U.S. embarrassment at the leaked SIPRnet cables was probably not so much due to wiki technology, as to inadequate internal computerised auditing and security controls in the U.S. military.

Finally, if in this new phase of the digital revolution self-regulation cannot prevent community harm or risks to national security, there may be grounds for internationally regulating wikis and so-called 'mirror' sites. While a detailed analysis of these issues is beyond the scope of this paper, they represent demonstrably fruitful avenues for future research in IT law and policy.

---

lascivious, filthy, excessively violent, harassing, or otherwise objectionable" would be neither liable civilly, nor liable under State criminal law: 47 USC § 230(c)(2)(a), (e)(3).

References

Australian Treaty Series (2002a), International Convention for the Suppression of Terrorist Bombings [2002] ATS 17.

Australian Treaty Series (2002b), International Convention for the Suppression of the Financing of Terrorism [2002] ATS 23.

Australian Treaty Series (2002c), International Convention for the Suppression of Acts of Nuclear Terrorism [2012] ATS 13.

Bean, L. and Hott, D.D. (2005), "Wiki: A Speedy New Tool to Manage Projects", *Journal of Corporate Accounting and Finance*, Vol. 16, Issue 5, pp. 3-8.

Benkler,Y. (2011), "A Free Irresponsible Press: WikiLeaks and the Battle over the Soul of the Networked Fourth Estate", *Harvard Civil Rights-Civil Liberties Law Review,* Vol. 46, pp. 311-397.

Brunton (2011), "WikiLeaks and the Assange Papers", *Radical Philosophy,* Vol. 166, pp. 8-20.

Burns, A.R. (1936), *The Decline of Competition*, New York: McGraw-Hill.

Cabranes, J.A. (2009), "Our Imperial Criminal Procedure: Problems in the Extraterritorial Application of US Constitutional Law", Yale Law Journal, Vol. 118, pp. 1660-1711.

Commonwealth of Australia (2010), Counter-Terrorism White Paper: Securing Australia, Protecting Our Community, Canberra: Department of Prime Minister and Cabinet.

Depoorter, B. and de Mot, J. (2006), "Whistleblowing: An Economic Analysis of the False Claims Act", *Supreme Court Economic Review,* 14: 135-162

Domscheit-Berg, D. (2011), *Inside Wikileaks*, New York: Crown (Random House).

Elsea, J.K. (2011), "Criminal Prohibitions on the Publication of Classified Defense Information", Congressional Research Service, Paper No. 7-5700 (R41404), Prepared for Members and Committees of Congress, 8 September.

Fenster, M. (2012), "Disclosure's Effects: WikiLeaks and Transparency", *Iowa Law Review*, Vol. 97, pp. 753-807.

Gardner T.J. and Anderson T.M. (2011), *Criminal Law*, 11th ed., Stamford Conn.: Wadsworth (Cengage).

Green, A. (2012), "Silence in the Courtroom", *Law and Literature,* Vol. 24(1), pp. 80-101.

Greer, C. and McLaughlin E. (2012), "This Is Not Justice", *British Journal of Criminology*, Vol. 52, pp. 274-293.

Hasan, H. and Pfaff, C.C. (2006), "The Wiki: An Environment to Revolutionise Employees' Interaction with Corporate Knowledge", Proceedings of the 18th Australia conference on Computer-Human Interaction: Design: Activities, Artefacts and Environments, November 20-24, Sydney.

Hicks, D. (2010), *Guantanamo: My Journey*, Sydney: Random House.

Jones S. and Ward Brown, J. (2011), "'The Assange Effect': WikiLeaks, the Espionage Act, and the Fourth Estate", *Media LawResource Center Bulletin*, Vol. 2, August. Available at: www.lskslaw.com/documents/WikiArticle(00445013).PDF *(Accessed April 17, 2012).*

Joseph, S. (2012), "Social Media, Political Change, and Human Rights", *Boston College International and Comparative Law Review*, Vol. 35 (1), pp. 145-188.

Macey, J. (2007) "Getting the Word out about Fraud: A Theoretical Analysis of Whistleblowing and Insider Trading", *Michigan Law Review*, 105: 1899-1940.

Moore, A.D. (2011), ""Privacy, Security, and Government Surveillance: Wikileaks and the New Accountability", *Public Affairs Quarterly*, Vol. 25, No. 2, April, p. 141.

Neuman G.L. (1991), "Whose Constitution?", *Yale Law Journal*, Vol. 100, p. 909-991.

Opper, M.H. (2011), "WikiLeaks: Balancing First Amendment Rights with National Security", *Loyola of Los Angeles Entertainment Law Review*, Vo. 31, pp. 237-267.

Oxford Dictionary (2010), Oxford University Press: Oxford. Available at: http://oxforddictionaries.com/definition/wiki (Accessed April 17, 2012).

Papandrea M. (2007), "Lapdogs, Watchdogs and Scapegoats": The Press and National Security Information", *Indiana Law Journal*, Vol. 83, pp. 233-305.

Silver, D.A. (2008), "National Security and the Press: The Government's Ability to Prosecute Journalists for the Possession or Publication of National Security Information", *Communication Law and Policy*, Vol. 13, pp. 448-483.

Stern S. (2007), "Constructive Knowledge, Probable Cause and Administrative Decision-Making", *Notre Dame Law Journal*, Vol. 82, pp. 1085-1142.

Stone, G.R. (2004), *Perilous Times: Free Speech in Wartimes from the Sedition Act of 1789 to the War on Terrorism*, New York: WW Norton and Co.

Stone, G.R. (2011), "WikiLeaks, the Proposed SHIELD Act, and the First Amendment", *Journal of National Security Law and Policy*, Vol. 5, pp. 105-118.

United Nations, *Multilateral Convention to Prevent and Punish the Acts of Terrorism taking the forms of Crimes against Persons and Related Extortion that are of International Significance*, A-49, Washington DC, signed 2 February 1971; Registered with UN 20 March 1989, No. 24381, OAS; Last updated 7 November 2007. Available at: http://www.oas.org/juridico/english/treaties/a-49.html (Accessed 17 April 2012).

Newspaper and Media

Adams, J. (2010, "Did Wiki Leaks Founder Julian Sons Commit a Crime?", *The Christian Science Monitor*, November 30.

Addley, E. (2011), "WikiLeaks: Julian Assange 'Faces Execution or Guantanamo Detention'", *The Guardian* (UK), 11 January.

Cloud, D.S. (2011), "Soldier in WikiLeaks Case Charged with Aiding the Enemy", *Los Angeles Times*, 3 March.

Davies, N. (2010), "10 days in Sweden: The Full Allegations against Julian Assange", *The Guardian* (UK), 17 December.

Dorling, P. (2012), "'Reckless' WikiLeaks Faces Fresh Fire from Canberra", *Sydney Morning Herald*, 31 March.

Fadel, L. (2010), "Army Intelligence Analyst Charged in WikiLeaks Case", *Washington Post*, 7 July.

Fowler, A. (2011a), "Wiki Whacked", *Foreign Correspondent*, Australian Broadcasting Corporation, 4 October. Available at: http://www.abc.net.au/foreign/content/2011/s3332165.htm (Accessed 19 April 2012).

Fowler, A. (2011b), "Wikileaks 'Architect' Threatens Site's Future", *ABC News*, Australian Broadcasting Corporation, 5 October. Available at: http://www.abc.net.au/news/2011-10-04/wikileaks-architect/3207748 (Accessed 19 April 2012).

Haynes, J. (2010), "Paypal Freezes WikiLeaks Account", *The Guardian* (UK), 4 December.

Lagan, B. (2010), "International Man of Mystery", *Sydney Morning Herald*, 10 April.

Leigh D, Harding L, Hirsch A, and MacASkill E. (2010), "WikiLeaks: Interpol Issues Wanted Notice for Julian Assange", *The Guardian* (UK), 30 November.

Leuf, B. and Cunningham, W. (2001). *The Wiki Way: Collaboration and Sharing on the Internet*, Reading, MA: Addison-Wesley.

Lucas D. (2012), "Julian Assange Prepares His Next Move", *Salon*, 24 February. Available at http://www.salon.com/writer/douglas_lucas/ (Accessed 30 April 2012).

MacAskill E. (2010), "WikiLeaks Website Pulled by Amazon after US Political Pressure", *The Guardian* (UK), 2 December.

MacAskill E. (2010), "Julian Assange like a High-Tech Terrorist, says Joe Biden", *The Guardian* (UK), 18 December.

Robinson, J. (2012), "Time for Government to Stand Ground and Protect Assange", *Sydney Morning Herald*, 1 March.

Rundle, G. (2010), “Did He or Didn't He? The Murky Politics of Sex and Consent ”, *Sydney Morning Herald*, 12 December.

Traynor, I. (2010), “WikiLeaks founder Julian Assange Breaks Cover but will Avoid America”, *The Guardian* (UK), 21 June.

Welch, D. (2010), “Julian Assange has Committed No Crime in Australia: AFP”, *Sydney Morning Herald*, 17 December.