Changing Paradigms of Media Landscape

In The Digital Age: Issue and Perspectives (Rise of Social Media)

- Digital Media Vs Traditional Media
- Digital Media: Scope & Challenges
- Media and Democracy
- Digital Media and Ethics
- Digital Media and Governance
- Digital Media vis-à-vis Laws & Regulations
- Digital Media as Community Media
- Digital Media and Contemporary Cinema

AMITY SCHOOL of COMMUNICATION
www.amity.edu/jaipur
A Survey Analysis of Digital Literacy among undergraduate Students of the University of Tehran
Hamid Abdollahyan and Mohammad Ahmadi

From Disney to Doraemon: Japanese Anime substitute American Animation on Indian Children’s Television: A trend study
Ruchi Jagg

Digital Technology and The Challenges of Media Literacy in A Developing Nation
Yomi Olugbodi

Activist Living: Professional and Economic Renewal for Journalism in the Age of Digital Media
Bradley Clark

Dominance of Digital Media over Traditional Media: A critical study
B.K.Ravi

Factors Influencing Proliferation of Digital Media in a Formal Group: A Dynamic Perspective
Rahul Thakurta

Internet and Political Change in Iran: Nature or Content?
Ehsan Shaghasemi and Tiba Bonyad

Executive Blogging: What Do Indian Corporate Heads Blog About and Why?
Sneeta Mishra

Media Regulation Vs Democratic Values In India
Pallavi Majumdar

Communication for Affiliation: An Indicative Approach to Understand Blogging
Vikas Dogra and Manish Verma

U.S. Business : Tort Liability for the Transnational Republisher of Leaked Corporate Secrets
Richard J. Peltz

Mobile Journalism (MOJO) : Origin and Spread Around the World
Stephen Quinn

UGC in the American and Arab Media Websites
Elsayed bekhit

Book Review
- Private Sphere: Democracy in a Digital Age (Digital Media and Society)
  Jayati M. Sharma
- Media in the Digital Age
  Tanushree Mukherjee
U.S. Business: Tort Liability for the Transnational Republisher of Leaked Corporate Secrets

Richard J. Peltz
University of Arkansas, USA

Wikileaks, the web enterprise responsible for the unprecedented publication of hundreds of thousands of classified government records, is reshaping fundamental notions of the freedom of information. Meanwhile more than half of records held by Wikileaks are from the private sector, and the organization has promised blockbuster revelations about major commercial players such as big banks and oil companies. This paper examines the potential liability under U.S. business-tort law for Wikileaks as a transnational republisher of leaked corporate secrets. The paper examines the paradigm for criminal liability under the Espionage Act to imagine a construct of civil liability for tortious interference with prospective economic relations; considering key problems of scienter, jurisdiction, and constitutionality. The paper concludes that prospects for civil liability are dim.

Keywords: Business torts, espionage, freedom of information, secrecy, tortious interference, wikileaks

Introduction

Wikileaks, the organization responsible for the controversial 2010 Internet publication of Afghanistan and Iraq “war logs” and a cache of U.S. diplomatic cables challenges the fundamental ideal of freedom of information with an unprecedented expression of absolutism. After the cables release, which began in November 2010 and is ongoing, the U.S. Attorney General opened a criminal investigation into Wikileaks. Constitutional scholars and civil liberties advocates were quick to caution against the imposition of criminal liability for the publication of government secrets by an organization purportedly in the business of journalism, in contrast with, namely, Bradley Manning, the U.S. Army intelligence analyst charged with leaking the classified records to begin with. Indeed, criminal prosecution of Wikileaks would occasion formidable legal obstacles, broadly an ill fit between classic espionage laws and a mass media defendant.

Meanwhile, a less well examined but equally important problem is potential civil liability for Wikileaks. Wikileaks disclosures range well beyond the big splashes of U.S. governmental records and include important private-sector content such as embarrassing revelations from within Iceland’s embattled Kaupthing Bank (Bowers, 2009). According to flamboyant Wikileaks spokesperson Julian Assange, Wikileaks possesses as-yet unreleased stores of documents unflatteringly revealing of corporate misconduct within such prominent targets as global banks and oil companies (Greenberg, 2010). A host of liability theories may be leveled against Wikileaks upon the revelation of corporate secrets, but civil liability comprises a much murkier proposition than criminal prosecution. Thus the threat of civil liability poses questions integral to the maturation of freedom of information as a human rights norm.

This paper explains what Wikileaks is, and then traces the contours of civil liability exposure on U.S. business torts for the transnational publisher of truthful, leaked information, with emphasis on the tort of intentional interference with prospective economic relations. Wikileaks may be hailed into court around the world, but this paper focuses on U.S. law because it has been a bellwether in the development of norms governing the interaction of human rights and tort law. Because the law in this area, in the United States as elsewhere, is too uncertain to dictate a result on the merits, this paper examines the problem of criminal prosecution before considering civil liability. Criminal prosecution has been better examined to date, and the impediments that have been identified have civil analogs. Considering the impediments in the civil context, the paper concludes that prospects for a successful civil suit are dim.

About Wikileaks

Launched in 2006, Wikileaks is a loose, largely anonymous, and international association of advocates for freedom of information in the public interest. The organization’s ranks include a small
core staff and a network of volunteers around the world, principally journalists and hackers (Mey, 2010). Funded by donations, WikiLeaks employs military-grade encryption to safeguard data on servers in various locations, including Sweden and Switzerland (Greenberg, 2010; Mey, 2010). Presently centered at the Swiss site “wikileaks.ch,” WikiLeaks located its physical operations within legal jurisdictions that place high value on the journalist-source privilege and that observe content-neutral, non-interventionist policies with respect to Internet service providers and the content they carry (Helin, 2010; Bränstad, 2010).

WikiLeaks collects information through an online “drop box”; as a matter of policy, if arguably of practice, WikiLeaks does not solicit contributions (Bränstad, 2010). Any person with Internet access can submit data anonymously to WikiLeaks via the website. WikiLeaks promises anonymity to its sources and pledges to the public that it will post only unfiltered and authentic content of “political, ethical, diplomatic or historical significance” (WikiLeaks, 2010). Initially conceived as a “wiki,” WikiLeaks in fact abandoned the public-participatory model in 2010 in favor of coordinated publications with traditional media outlets given advance access on condition of embargo (Gilson, 2010; Ellison, 2011). Though driven to international repute by the war log and cable releases of 2010, WikiLeaks engages as well in high-profile releases of private-sector records. Julian Assange, a co-founder and iconic spokesman for WikiLeaks, has advocated freedom of information absolutism, though WikiLeaks has redacted sensitive information such as the identities of informants from the Iraq war logs (Bränstad, 2010).

The Paradigm of Criminal Liability

While this paper seeks to examine civil liability for U.S. business torts, the well examined prospect of U.S. criminal prosecution has generated a rubric of legal impediments with civil analogs. Thus an analysis of the criminal paradigm is a logical precursor to construction of the civil paradigm.

When the Afghan war logs went live on WikiLeaks, the Pentagon futilely demanded the return of leaked records (Bränstad, 2010) and quickly identified and detained the probable military source of the leak (Hodge, 2010). When later in 2010 the U.S. Administration was embarrassed by the revelation of the diplomatic cables, the civilian government was compelled to respond. U.S. Attorney General Eric Holder opened an investigation into WikiLeaks. Upon objections by civil liberties advocates that the U.S. Espionage Act had never been used to prosecute a mass media publisher, Holder indicated that WikiLeaks would be investigated under various statutes (Savage, 2010).

Holder was tight-lipped on the details, but the Congressional Research Service (CRS) published a thorough examination of potential criminal responsibility for WikiLeaks (Elsea, 2010). In sum, CRS was highly skeptical that a criminal prosecution could succeed. The impediments to prosecution that CRS identified can be restated in three categories: (1) scint, (2) extraterritoriality and jurisdiction, and (3) constitutionality. While specific analyses vary with statutes, almost all wreck on the shoals of these impediments.

The Espionage Act of 1917, 18 U.S.C. §§ 792-799 (2011), is illustrative. With regard to scint, the Espionage Act requires intent. The key provisions of the act confront prosecutors with a series of hurdles. For example, section 793 prohibits taking, copying, receiving, or obtaining “national defense” information with “intent or reason to believe that the information is to be used to the injury of the United States.” Thus intent pertains to acquisition of the information; to the content as “defense” information; and (with a “belief” alternative) to injurious motive. Section 793 separately criminalizes disclosure to “an unauthorized person,” thus another intent hurdle vis-à-vis the publisher-defendant.

These requirements are well suited to a classic spying case; they ill fit WikiLeaks (Elsea, 2010). First, the passive WikiLeaks drop box does not plainly establish intent to take, copy, or obtain information. Even as to receipt, it is difficult to pinpoint the time at which WikiLeaks formulated intent. The drop box came into existence at an indefinite time before the information was actually delivered; actus reus only arguably occurs through the sudden electronic “possession” of submissions by automated servers. More problematically, the passive drop box renders intent hard to prove as to content. WikiLeaks readily confesses a desire to receive information not yet public from all sectors, but arguably manifests no intent specific to “national defense.” Similarly, mass dissemination evinces no intent specific to injury to national interests; to the contrary, WikiLeaks purports to further national interests by disseminating information to the democratic electorate. Arguably, reckless disregard of injurious potential describes the WikiLeaks state of mind at its
most culpable, manifested for example in the outing of Afghan informants before Wikileaks adopted a reduction policy (Bråstad, 2010).

Before the Government can make its case on scintener, there are practical problems attending extraterritorial application of the Espionage Act and the jurisdiction of U.S. courts. On the face of the matter, these problems are surmountable. Jurisdiction would depend on the United States securing an agent of Wikileaks personally in U.S. custody. The problem is a practical one. Assange, who is Australian, has avoided U.S. jurisdictions assiduously since the summer of 2010 (Wikileaks founder, 2010). He has warily regarded Sweden’s attempts to secure his extradition from Britain, in a criminal investigation purportedly unrelated to Wikileaks, as a first step toward extradition to the United States (Wigglesworth & Satter, 2010). Meanwhile extraterritorial application of U.S. statutes is dependent on legislative intent. CRS concluded that such intent is adequately manifested in the Espionage Act by the 1961 repeal of provisions limiting the act to application in domestic law and admiralty (Elsea, 2010). Accordingly, a federal court in the 1980s accepted the guilty plea of an East German defendant for espionage abroad (U.S. v. Zehe, 1985).

Still, there might be a problematic dimension to the purely extraterritorial application of espionage law. CRS reasoned that espionage laws are, in overarching purpose, treason laws (Elsea, 2010). Treason arises from the defendant’s betrayal of a duty of loyalty to nation; Assange has no such duty to the United States. If a rank-and-file analyst in the Iranian foreign intelligence service passes an unlawfully intercepted U.S. diplomatic communication to a Tehran officemate, neither of the two is guilty of “treason,” any more than their counterparts in Langley can be said daily to commit treason against foreign nations. There must be some outer limit to the purely extraterritorial application of espionage law, and that limit might save Wikileaks.

Problems of scintener, extraterritoriality, and jurisdiction all surmounted, a final and most likely prohibitive barrier to criminal prosecution derives from the affirmative defense of freedom of expression. As CRS explained simply, espionage laws have not before been used to condemn mass media (Elsea, 2010). The Wikileaks case might exemplify the U.S. Supreme Court disinclination to punish the republication of truthful information lawfully obtained. Where, for example, a reporter obtained and published the name of a sexual assault victim released by police in inadvertent violation of state law, the Court disallowed punishment of the reporter (Florida Star v. BJF, 1989). Where statutes outright forbade the publication of the name of a sexual assault victim, or of a juvenile charged with a crime, the Court ruled them unconstitutional (Cox v. Cohn, 1975; Smith v. Daily Mail, 1979). The Court has left the door open to such a prosecution, but never decided the case. Constitutional muster would not be met easily. In strict scrutiny of a Wikileaks prosecution, tighter government security in the first place, or prosecution of the military leaker, are readily available alternatives, less restrictive of free expression than criminal prosecution of the mass media republisher. Thus prosecution would fail strict scrutiny.

Perhaps instructive on the free expression question is a 2006 federal case involving the American Israel Public Affairs Committee (AIPAC) (U.S. v. Rosen, 2009). Two pro-Israel lobbyists in the United States were indicted for conspiracy to disclose national defense information to the government of Israel and to a reporter for The Washington Post newspaper. Federal prosecutors ultimately dropped the charges (NAA, 2009); the court had expressed serious reservations about the Government’s ability to meet the demanding intent hurdles of the Espionage Act (U.S. v. Rosen, 2006). But CRS offered an even more salient assessment of AIPAC and its relevance to Wikileaks: in the first ever prosecution under the Espionage Act of civilians in the private sector, the government suffered powerful reproach for “criminalizing the exchange of information” (Elsea, 2010, p. 9). The relationship of Wikileaks to prominent global news outlets such as The New York Times and The Guardian would render comparison inevitable between Wikileaks and AIPAC. Even without clear legal precedent on the applicability of espionage law in such a case, the government might be unable to advance a prosecution against crushing opposition in the political sphere, where mass media protest would rally public opinion.

Another potentially derailing parallel runs between Wikileaks and New York Times v. United States (the Pentagon Papers case, 1971), which involved the leak by military contractor Daniel Ellsberg of classified and embarrassing revelations about U.S. involvement in Vietnam. PFC Manning, not Wikileaks, is the Ellsberg analog here. The Ellsberg prosecution failed upon the revelation of troubling conduct by government investigators, such as illegal wiretaps, not likely to be an
impediment in the court martial of Manning. In Pentagon Papers, the U.S. Supreme Court upheld the free expression rule against prior restraint, rejecting an injunction against republication. Though Pentagon Papers was a case of prior restraint and not a case of punishment ex post, the factual parallels are striking. It is difficult to ignore that prosecution of the Times for publication of the Pentagon Papers would have resulted in subsequent "self-censorship," thus prior restraint in practical effect. If Pentagon Papers is an applicable precedent for Wikileaks, then the analysis for the constitutional defense might demand even more than strict scrutiny, for example, that the defendant actually jeopardized lives by publishing troop movements in advance. One can argue that a very small segment of Wikileaks war-related releases meet that standard—e.g., the Afghan informants' identities, or tactical strategies for urban combat—but no release has yet been tied causally to a casualty.

Perhaps the best prospect identified by CRS (Elsea, 2010) for a successful criminal prosecution of Wikileaks lies in charges for theft of government records (18 U.S.C. § 641). If Wikileaks does not demonstrate an adequate combination of actus reus and mens rea to be guilty of espionage, the case for theft of government property is more daunting. Like the common law offense of receiving stolen property, intentionality occurs in the receipt; the crime is then accomplished by mere knowledge of the predicate theft, or reason to believe it occurred. When Wikileaks collects the fruits of its drop box and then hears the Pentagon demand for the return of stolen property, the theft appears complete. But prosecution for theft has an important limitation in remedy. Copies of electronic records have no tangible value, so financial restitution approaches zero. Maximum penalties for such petit larceny are a modest fine and a year's imprisonment; hardly the newsworthy triumph that would justify a substantial deployment of government resources in the politically dubious prosecution of an elusive international entity.

Wikileaks is therefore hardly immune to criminal prosecution in the United States for its activities. But the obstacles to a successful prosecution, including the practical, legal, and political, are overwhelming. These same variables come into play in the civil context.

**Imagining Civil Liability**

Western media have focused on the war and cable releases, but those records comprise only fraction of Wikileaks secrets. Since 2003, Wikileaks has made splashes around the world with releases of public significance and private-sector authorship, including, in 2007, records of politically motivated murders in Kenya; in 2008, secret documents of the Church of Scientology, the membership of the far-right British National Party, and e-mails from the personal account of U.S. vice presidential candidate Sarah Palin; and in 2009, records of an oil scandal in Peru and of shenanigans inside banks such as Kaupthing, which decimated the Icelandic economy (Greenberg, 2010; Kushner, 2010). In December 2010, Wikileaks spokesperson Julian Assange asserted that Wikileaks is still safeguarding the embarrassing secrets of big banks, possibly including the Bank of America; big pharmaceutical companies; and big oil companies, including BP, the company blamed for the 2010 oil spill in the Gulf of Mexico (Greenberg, 2010). Thus with more revelations from the private sector on the horizon for 2011 and coming years, and the prospects for criminal prosecution limited, civil lawsuits in the United States and elsewhere seem inevitable (Savage, 2010).

Wikileaks has been sued civilly once already in the United States by the victim of a leak (Bank Julius Baer v. Wikileaks, 2008). Records posted in 2008 evidenced suspicious financial transactions in the Cayman Islands branch of the Swiss bank Julius Baer. Realizing that its dirty laundry was on public display, Baer Bank moved quickly to obtain an injunction from a U.S. federal court in California, to shut down the Wikileaks domain “wikileaks.org.” The bank sued both Wikileaks and its California Internet service provider, Dynadot. Dynadot negotiated a settlement with the plaintiff to shut down the domain. Wikileaks did not appear, and the trial court entered a purportedly stipulated, permanent injunction upon the settlement. But the bank’s victory was hollow. In anticipation of the court order, websites around the world mirrored wikileaks.org. Meanwhile, amici, including top mass media in the United States, urged the court to reconsider in light of free expression. Ultimately the court rescinded the injunction, citing both free expression and futility, and Baer Bank learned a hard lesson on the “Streisand effect”: the ironic tendency of the Internet to amplify the distribution of information that someone tries to squelch. The effect is named for diva Barbara Streisand, whose multi-million-dollar lawsuit against a photographer catapulted his image of her coastal estate into stratospheric circulation.
Though Baer Bank amounted to no decision on the merits, the lawsuit cataloged pertinent common law tort actions: interference with contract, interference with prospective economic advantage, and conversion. Baer Bank furthermore alleged violations of unfair business practices, consumer banking, and privacy protection laws. One can imagine as well a statutory action for copyright infringement (Savage, 2010), essentially a conversion of intellectual property. These civil causes raise the same triad of problems as in the criminal arena: scienter, extraterritoriality and jurisdiction, and constitutionality. How these causes would fare against these problems is even less clear than in the context of criminal sanction, for want of precedents, though a successful suit in sum seems unlikely.

Exemplary is the common law tort for intentional interference with prospective economic advantage, very similar and slightly more permissive than interference with contract. The common law elements are: (1) the existence of an economic relationship between plaintiff and a third party; (2) defendant’s knowledge of the relationship; (3) defendant’s wrongful and intentional interference with the relationship; and (4) resulting damages (Muskus, 2010).

The scienter problem is akin to that presented under the Espionage Act, which is to say, it is not clear that mass media dissemination can suffice as an intentionally interfering act. Baer Bank, for example, would have maintained that Wikileaks intentionally interfered with the bank’s relationships with clients or investors. But as CRS observed with respect to criminal prosecution under espionage law (Elsea, 2010), the cause conventionally has not been used to target mass media not themselves complicit in the predicate leak. In one high-profile case, for example, professional basketball player Latrell Sprewell complained to New York courts that the New York Post interfered with his employment by reporting that he had broken his hand in a fight, not in a fall as he had reported (Kovner, et al., 2010). The court dismissed the interference claim, opining that “[a]ny interference was entirely incidental to the defendants’ exercise of their constitutional right to [publish] newsworthy information” (Kovner, et al., 2010, p. 387).

Also like in the criminal analysis, the problem of jurisdiction is surmountable in theory but challenging in practice. Extraterritoriality is not the problem that it is in the criminal arena, because the defendant is present in the United States and suffers its alleged injuries there. A case might falter, though, on jurisdiction. Extradition is of course not available to a civil plaintiff, so Wikileaks and its agents may rely on the security of protective laws where its operations are located in Sweden and Switzerland, and in the future perhaps Iceland, where outrage over Kaupthing Bank revelations has prompted a movement toward legal sanctuary for the free flow of information (Greenberg, 2010). Baer Bank asserted that Wikileaks maintained a personal presence in California, but proffered no evidence to that effect.

Finally, the constitutional problem is again likely prohibitive. At the outset of the analysis of the tort on the elements, concern for the freedom of expression puts a thumb on the scale for the defendant in at least two respects. First, the court’s decision in Sprewell, for example, rejected intent with reference to the “constitutional right to [publish] newsworthy information.” Typically in U.S. tort law, recklessness comes close enough to intent to short circuit the analysis, where the civil standard for intent is looser than the stringent mens rea analysis of criminal law. But Wikileaks’s possible recklessness did not make the cut, suggesting the pressure of free expression-friendly public policy. Second, tortious interference requires “wrongful” or “improper” intentional interference, and that requirement is similarly mitigated by public policy. Impropriety is determined with reference to six factors: (a) the nature of the defendant’s conduct, (b) the defendant’s motive, (c) the interests of the plaintiff with which the defendant interferes; (d) the interests sought to be advanced by the defendant, (e) the social interests in protecting the freedom of action of the defendant and the economic interests of the plaintiff, (f) the proximity or remoteness of the defendant’s conduct to the interference, and (g) the relations between the parties (ALI, Restatement § 767, 2010). These factors amply permit a court to consider the protection of free expression and the relative merits of freedom of information vis-à-vis secrecy. A seemingly corrupt corporation as plaintiff is highly unlikely to prevail against a mass media organization acting without profit motive and purporting to act in the public interest.

The thrust of the constitutional analysis comes moreover in the assertion of the freedom of expression as an affirmative defense. The impact of that assertion in a case of tortious interference is unclear, with precedents pull in opposite directions. On the one hand is the doctrine broadly identified
with New York Times Co. v. Sullivan (1964) in the defamation area. The Sullivan doctrine dramatically limits the potential for tort recovery against a media defendant in most cases of public import by imposing special rules, both procedural and substantive, particularly elevation of the requisite standard of fault to “actual malice.” Actual malice means actual knowledge of falsity or reckless disregard of falsity and is construed as more stringent than ordinary recklessness in tort, if just shy of intent. Critically, Sullivan prohibits liability for the publication of truth, shifting the burden of proving falsity to the defamation plaintiff. The U.S. Supreme Court has extended the Sullivan doctrine to the torts of false light invasion of privacy and intentional infliction of emotional distress, opining that the protection of Sullivan for free expression should not be subverted through careful pleading. But the Court has not opined on the application of Sullivan to torts such as negligent disclosure invasion of privacy, nor tortious interference with contract. Significantly in those torts, the publication of truth, and not the commission of a fraud, is the very thing that makes the defendant's conduct injurious. How Sullivan would change the analysis on those torts is unclear.

The opposing line of precedents may be defined broadly by Branzburg v. Hayes (1972). In Branzburg, the U.S. Supreme Court rejected a journalist’s privilege as a matter of constitutional imperative. Where journalists were called to give evidence to grand juries, the Court reaffirmed the doctrine that generally applicable rules of law apply to journalists just as to anyone else. The right of free expression might bear on the propriety of a subpoena, but compels no recognition of a journalist-source privilege not otherwise provided by common law or statute. More broadly, then, Branzburg stands for the proposition that there is no constitutional right to gather news. If Branzburg is the appropriate lens through which to view a mass media defendant alleged to have interfered tortiously with prospective economic advantage, or for that matter a mass media defendant accused of negligently disclosing information and thereby invading a plaintiff's privacy, then the defendant is entitled to no constitutionally based privilege and is subject to liability on the same terms as any person.

When the Baer Bank court rescinded its injunction against Wikileaks, the court based its decision in part on constitutional concerns and, without plainly citing the freedom of expression, seemed to invoke a heightened constitutional scrutiny known to injunction law and derived from the law of prior restraint. The injunction was problematic under the court’s own analysis, in large measure because of the futility problem. An order against free expression must directly advance the government interest at stake, and the court’s order had the opposite effect, only exaggerating the mass dissemination of Baer Bank’s secrets. Significantly, then, civil remedies against Wikileaks will be difficult to justify if any heightened constitutional scrutiny applies, whether under the Sullivan framework or under the prior restraint framework.

Therefore like the espionage law, tortious interference is simply a bad fit with Wikileaks. The criminal paradigm is instructive again in finding a better prospect for civil recovery against Wikileaks in the simple tort of conversion. Conversion in common law (ALI, Restatement § 222A) is loosely construed to permit liability even where the defendant's use of property has interfered with the property rights of the owner, short of a complete taking, and the requisite intent arises simply from the taking or use. But conversion poses serious limitations analogous to those presented by the prospect of criminal prosecution for theft of property. Damages are limited to the actual value of the property loss/approaching zero where electronic records have been copied and consequential special damages. As a matter of legal cause, beyond mere factual cause, injury to the reputation of Baer Bank, for example, seems fairly traceable only to the financial irregularities that were exposed, not to the act of leaking the records, let alone republishing records already leaked. Perhaps more importantly, again as in the criminal analysis, a conversion plaintiff seeking a modest recovery would have to consider the countervailing political cost in public opinion, magnified by the Streisand effect.

Conclusion

The Hollywood movie The Insider (Brugge, 1999) told the true story of the U.S. newsmagazine 60 Minutes, threatened with liability for tortious interference for publication of an interview with a Big Tobacco whistleblower. When in the fictionalized version of events the broadcast network counsel explained that the truth of the publication in fact determined the quantum of damages, the reporter played by Al Pacino asked, “Is this Alice in Wonderland?” Indeed, the prospect of criminal prosecution or civil liability for the publication of truthful information lawfully obtained seems inconsistent with human rights norms in the freedom of expression and the free flow of information.
But WikiLeaks poses an unprecedented test to the latter half of the maxim "lawfully obtained" and presents open questions as to the legal responsibility of the mass media recipient and republisher of leaked information. The prospect of espionage prosecution in the United States for the revelation of government secrets is likely to run aground on the shoals of scienter, extraterritoriality and jurisdiction, and constitutionality. At best the government might prosecute successfully for theft, but that prosecution promises limited remedies and possibly prohibitive political costs. The prospect for business tort liability in the United States for the revelation of business secrets seems faint analogously upon problems of scienter, jurisdiction, and especially constitutionality, though the applicability of precedents is far from certain. Like in the criminal area, a civil suit for conversion seems more promising, but poses possibly prohibitive reputational risks for would-be plaintiffs. In sum, dim prospect for civil liability counsel caution to corporations in the maintenance and management of secrets.

It merits consideration that this study of potential U.S. business tort liability for an entity such as WikiLeaks bears important limitations. This paper on business tort liability did not examine ancillary tort doctrines such as civil conspiracy. More importantly, this paper examined only business tort liability in the United States. Civil liability regimes vary greatly around the world, and WikiLeaks might as likely be haled into court anywhere a business suffers reputational harm. Moreover, other legal regimes have rejected the constitutional doctrines of both Sullivan, as overprotective of free expression, and Brandenburg, as under-protective of free expression. Thus a comprehensive picture of civil exposure worldwide for WikiLeaks demands further research.

References


Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (1975).


