The John Marshall Journal of Information Technology & Privacy Law

Volume 31 | Issue 3 Article 3

2014

Beyond Privacy Rights: Crossborder Cyber-Espionage and International Law, 31 J. Marshall J. Info. Tech. & Privacy L. 369 (2014)

Stefan Kirchner

BEYOND PRIVACY RIGHTS: CROSS-BORDER CYBER-ESPIONAGE AND INTERNATIONAL LAW

STEFAN KIRCHNER[1]

A. INTRODUCTION: DATA AS RAW MATERIAL FOR THE GLOBAL ECONOMY

There is a difference between voluntarily giving somebody an amount of money and having the same amount of money taken away from you, maybe even without noticing it at first. Even though the economic situation might be the same, it is the loss of control of sovereignty over one's own affairs, which we find troublesome. Likewise, hardly anyone, when buying something from a complete stranger, would assent to the idea that one is to hand over one's wallet, let the seller take whatever he or she sees fit, and return the wallet, with the buyer only being able to find out much later how much was taken. Yet, this is exactly what many of us consent to every day when we use the Internet.

We are used to the idea that a lot of the services and products offered on the Internet are free. Yet, from the perspective of economics, this makes little sense. Although there are of course cases of altruism, public service, and simply the interest in doing things, like writing a blog, cyberspace is also a commercial space. If you use a free service, you will usually find advertisements. Some advertisements will follow you around the net when you visit other websites. Some advertisements you will see because you had searched for a specific product or service online. This is only the beginning of targeted advertising. This requires data and it is this potential for commercialization, which makes data valuable. Data is the currency in which we pay for seemingly free Internet services. Indeed, we not only provide data as a form of payment, but often the ability to share data with others is the service. Essential-

1. Associate Professor for Fundamental and Human Rights, University of Lapland, Rovaniemi, Finland; admitted to the bar (*Rechtsanwalt*), Frankfurt am Main, Germany; Doctor in Social Sciences, Vytautas Magnus University, Kaunas, Lithuania; Magister Juris Internationalis, Justus-Liebig-University, Giessen, Germany.

ly, we pay with data for the ability to share data more effectively. This contributes to creating the impression for users that data is of little value. Yet, what is of little value to the user, and which might not even be perceived as data, can be valuable for companies.

A case in point is geodata. Today almost everybody's location can be found because we allow for it the moment we turn on a mobile phone. In the case of mobile phone services, the prices paid for the ability to communicate are both money and data. Until the revelations by Edward Snowden, this openness for sharing data has led to a lack of awareness of government entities' interest in data. Yet, the interest in using data-sharing services continues and data has become the new raw material on which a large part of the global economy is being built. As large transnational corporations are becoming too big to be regulated by a single nation state, states will develop an interest in data. This raises the question of the legality of state espionage targeting international telecommunications, Internet companies, and ultimately individual users.

But espionage is not limited to these sources. Espionage can also include the use of state-controlled assets for the purpose of gaining information from a corporation with the aim to improve the knowledge of a competitor based in one's own country.

States can now access information about individuals without any direct access to the individual by targeting social media websites. This does not actually have to be done by employing covert measures but can involve the use of domestic law to target corporations in order to get access to user data. In late 2014, this was taken one step further in two separate incidents.

In one incident unauthorized mobile phone base stations were discovered in the governmental quarter of the Norwegian capitol city of Oslo.[2] Later it was reported that Sweden and Finland had also been targeted.[3] These base stations enabled the perpetrators who remain unknown at the time of writing – to intercept mobile phone calls. Unlike cases of landline wiretapping, this affects everybody whose mobile phone logs in to one of these stations. Even without using a phone, this enabled the perpetrators to identify movement patters, although it appears likely that members or employees of government institutions were the intended targets.

The better known incident involved hackers of a group which calls itself "Guardians of Peace" (GOP), who are suspected of working for the

---

2. *Security Police: Phone Tapping also Occurred in Finland*, YLE UUTISET (Dec. 19, 2014),http://yle.fi/uutiset/security_police_phone_tapping_also_occurred_in_finland/7699262.

3. *Id*.

government of North Korea[4] and who targeted Sony corporate and employee data over a comedy movie in which the North Korean leader was portrayed by an actor in a work of fiction.[5] In combination with terrorist threats against cinemas in the United States,[6] this led to the decision not to screen the movie.[7] Compared to the Stuxnet attack against centrifuges in an Iranian nuclear research installation,[8] which led to the physical destruction of hardware through software manipulation,[9] the attack by North Korea has taken cyber warfare to a new level. This hacking attack provides the most recent, and arguably the most worrisome example of the impact of hacking on a society so far. It also makes it necessary to seek ways to utilize international law for the purpose of protecting individuals against such measures by (foreign) states.

In this text, we will look first at the regulation of espionage under international law in general before taking a closer look at selected aspects of international human rights law with the aim of identifying international rules which protect non-state actors against espionage by states be it the own state or a foreign country's government. In addition, the legal situation in the United States and Canada will be addressed. While global elements will be taken into account, the focus will be on European Human Rights Law as the European Convention on Human Rights (ECHR)[10] contains rights which can actually be claimed in the European Court of Human Rights and against parties to that Convention, other than those in which the victim is physically located.[11]

---

4. Alan Yuhas, *FBI Accuses North Korea of Hack*, GUARDIAN (Dec. 19, 2014, 11:49 AM), http://www.theguardian.com/us-news/live/2014/dec/19/obama-fbi-sony-hack-north-korea-china.

5. Dave Itzkoff, *Offended, Mr. Kim? Oops.*., N.Y. TIMES, Dec 21, 2014, at AR1, *available at* http://www.nytimes.com/2014/12/21/movies/james-franco-and-seth-rogen-talk-about-the-interview.html (the article's title in print and online are different).

6. Michael Cieply & Brooks Barnes, *Quandry for Sony in Threats Over Film*, N.Y. TIMES, Dec. 17 2014, at B1, *available at* http://www.nytimes.com/2014/12/17/business/media/sony-weights-terrorism-threat-against-opening-of-the-interview.html.

7. *New York Premier of Sony Film The Interview Cancelled*, BBC NEWS (Dec. 17, 2014, 6:47 AM), http://www.bbc.com/news/entertainment-arts-30507306.

8. Michael B. Kelley, *The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought*, BUS. INSIDER (Nov. 20, 2013, 12:58 PM), http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11?IR=T.

9. *Id.*

10. *Geneva Conventions*, INT'L COMM. RED CROSS, http://www.icrc.org/Web/Eng/siteeng0.nsf/html/genevaconventions (last visited Jan. 12, 2015).

11. Christoph Grabenwarter, EUROPEAN CONVENTION ON HUMAN RIGHTS, COMMENTARY 7 (C. H. Beck eds., 1st ed. 2014).

B. CLASSICAL INTERNATIONAL LAW: LIMITED REGULATION OF SPYING

I. ESPIONAGE UNDER INTERNATIONAL LAW

International law does not contain a general rule on espionage and only a limited number of codified rules.[12] Espionage between states is unfriendly[13] but not necessarily illegal *per se*.[14] There are, however, specific rules concerning espionage under specific conditions or "situation[s]."[15] In the following, these will be dealt with only briefly because these rules, as will be shown, are of little practical value for our search for legal protection of non-state victims against espionage.

The key difference is between the regulation of espionage in times of peace and in armed conflicts. Signal intelligence (sigint) plays an important role in both contexts. Espionage in times of peace is not necessarily prohibited, at least not by a peremptory norm[16] of international law.[17]

While international law, specifically the *ius ad bellum* – in principle, prohibits the use of armed force in international relations,[18] it also has a role to play when this fundamental rule has been broken, and it regulates the relations between the parties to a conflict, which has become an armed conflict, through the *ius in bello*, the laws of war, today often referred to as International Humanitarian Law.[19]

While espionage might be illegal, indeed a crime under most national legal systems,[20] it is not always illegal under International Humanitarian Law,[21] at least not if it is done by state actors. In other

---

12. Simon Chesterman, *The Spy Who Came in from the Cold War: Intelligence and International Law*, 27 MICH. J. INT'L L. 1072, 1072 (2006); JOHN KISH, INT'L LAW AND ESPIONAGE vii (Martinus Nijhoff Publishers ed. 1995).

13. *cf.* James P. Terry, *Book Review*, 9 DUKE J. COMP. & INT'L L. 491 (1999) (reviewing WALTER G. SHARP, CYBERSPACE AND THE USE OF FORCE (Aegis Res. Corp., 1st ed. 1999)); WALTER G. SHARP, CYBERSPACE AND THE USE OF FORCE (Aegis Res. Corp., 1st ed. 1999)).

14. *cf.* Kish, *supra* note 12, at xv.

15. Afsheen J. Radsan, *The Unresolved Equation of Espionage and International Law*, 28 MICH. J. INT'L L. 595, 606 (2007).

16. Vienna Convention on the Law of Treaties, arts. 53, 64 May 23, 1969, 1155 U.N.T.S. 331.

17. Roger D. Scott, *Territorially Intrusive Intelligence Collection and International Law*, 46 A.F.L. REV. 217, 218 (1999).

18. U.N. Charter art. 2, para. 4.

19. *See* Stefan Kirchner, *Modern International Humanitarian Law*, *in International Law: Contemporary Problems and Future Development* 231 (Sanford R. Silverburg eds. 2011).

20. Leslie C. Green, THE CONTEMPORARY LAW OF ARMED CONFLICT 120 (Manchester Univ. Press, 2nd ed. 2000).

21. *Id*.

words, those who are legally permitted to be combatants might, under Article 46 of Protocol I to the Geneva Conventions, in some cases also engage in espionage when they are identifiable as members of the armed forces of a party to an armed conflict,[22] *e.g.* if they wear uniforms while engaging in espionage[23] or if the espionage is undertaken by a member of the armed forces who is based ("resident") in an occupied territory.[24] The latter option is no longer technically necessary when it comes to espionage through the Internet and simply requires those manning the computers to wear uniforms while doing so.

II. CONSEQUENCES OF ESPIONAGE

In an armed conflict, spies might even, legally, create the illusion that they are "part of the enemy force."[25] Ruses are permissible under the laws of war while perfidy is outlawed.[26] Additionally, spies who are caught may not enjoy legal protection as prisoners of war.[27] International Humanitarian Law even allows the imposition of the death penalty for espionage,[28] although in many countries, national and international human rights law poses serious restrictions in this regard.[29]

But while spying is not always illegal, peacetime espionage can have consequences for interstate relations. This includes the practice of declaring spies, which have worked under the cover of diplomatic work *persona non grata* and asking them to leave the country.[30] While espionage is not necessarily illegal under international law, declaring a foreign diplomat who acted as a spy *persona non grata* is not merely an unfriendly act in reaction to the unfriendly act of espionage (and hence a retorsion), but also constitutes a legitimate reaction to the breach of either the Vienna Convention on Diplomatic Relations[31] or corresponding rules of customary international law, as the international legal

22. Torsten Stein & Christian von Buttlar, VÖLKERRECHT 446 (Carl Heymanns Verlag ed., 12th ed. 2009); JEAN-MARIE HENCKAERTS ET. AL., CUSTOMARY INTERNATIONAL HUMANITARIAN LAW 385 (Cambridge University Press, 1st ed. 2005); Radsan, *supra* note 15, at 601.

23. Green, *supra* note 20.

24. *Id*.

25. Gary D. Solis, THE LAW OF ARMED CONFLICT - INTERNATIONAL HUMANITARIAN LAW IN WAR 222, 430 (Cambridge Univ. Press 2010).

26. Green, *supra* note 20, at 146.

27. Solis, *supra* note 25, at 224, 430.

28. Green, *supra* note 20, at 150, 263.

29. Rhona K. M. Smith, TEXTBOOK ON INTERNATIONAL HUMAN RIGHTS 221 (Oxford Univ. Press, 6th ed. 2014).

30. Radsan, *supra* note 15, at 595, 621.

31. Vienna Convention on Diplomatic Relations, Apr. 18, 1961, T.I.A.S. 7502, 500 U.N.T.S. 95. For the field of consular relations see the Vienna Convention on Consular Relations, Apr. 24, 1963, T.I.A.S. 6802, 596 U.N.T.S. 331.

rules which govern diplomatic affairs do not allow for espionage by diplomats.[32] This not only follows from the doctrine of the prohibition of the abuse of rights but also from the purpose of diplomatic relations.

In the cases we are looking at in the context of this article, though, espionage is not necessarily conducted by diplomats – although there have been suspicions that diplomatic missions are being used for sigint purposes.

International treaties that regulate warfare have hardly kept pace with the technological developments of the last few decades. This is hardly a surprise because law often only has a chance to react and lawmakers will find it difficult to anticipate future challenges, especially in a field as rapidly developing as the Internet. Countries such as Georgia, Iran, or Estonia and countries which have suffered cyber-war attacks have not reacted with armed force, and *de lege lata* (*the view of the law*) a cyber-attack does not amount to an armed attack which would allow an armed response.

C. HUMAN RIGHTS

I. GENERAL REMARKS

In addition to these general considerations, human rights have to be taken into account when states take actions that affect non-state actors. This includes users but also corporations, which can also be holders of human rights.

As far as attempts by non-state actors to gain information are concerned, Article 19 of the Universal Declaration of Human Rights[33] provides a right to access information, albeit not one without limits. This limitation will usually provide a sufficient basis for data protection rules. It is, however, the obligation of the state to protect privacy rights through restrictions, which in turn must not lead to undue restrictions of the right of access to information.

II. THE PROTECTION OF PERSONAL DATA AS A HUMAN RIGHT UNDER ARTICLE 8 ECHR

Article 8 of the ECHR is far-reaching and protects a range of human rights, including the right to private life, which in itself has a wide scope. The focus of this investigation is the right to privacy, which is protected as part of the right to private life.

Already "the storage of information is capable of resulting in a

32. Radsan, *supra* note 15, at 595, 621.
33. UNIVERSAL DECLARATION OF HUM. RTS. art. 19.

breach of the right to respect for private life."[34] Accordingly, "[t]he registration of personal data has been a vital issue of the notion of privacy"[35] for the European Court of Human Rights.

Within the right to private life, the right to privacy is wide as well.[36] But at its core, "privacy, in its most obvious sense, connotes the capacity to keep certain information secret."[37] While it might be necessary to disclose specific information, which falls deeply within the realm of privacy,[38] such as an HIV infection,[39] the Convention places strict limitations on states when it comes to accessing such intimate information.

Sometimes, classical espionage methods are employed, for example when states spy on their citizens who have sought political asylum abroad. This does not have to involve any activities which are noticed by the victim and which may, as a result, be legal. For example, observing a building (which in the United States would not even trigger Fourth Amendment issues[40]) in order to find out who visits the building's residents. In the context of the Fourth Amendment, the valid expectation of the rights holder is an important factor in determining whether the material scope of the right to privacy is affected in the first place.[41] A similar test exists under Section 8 of the Charter of Rights and Freedoms of Canada,[42] although there are differences when it comes to the justifications of such searches.[43] "[A] reasonable expectation of privacy"[44] also exists beyond the home.[45] In the context of the European Convention on Human Rights, already the wide wording of Article 8 ECHR shows that privacy is multidimensional.

Under the European Convention on Human Rights the right to private life[46] also encompasses the protection of personal data.[47] This norm comes into play if the holder of the right is affected by the state's asking

---

34. Bernadette Rainey et al., THE EUROPEAN CONVENTION ON HUMAN RIGHTS 378 (Oxford Univ. Press, 6th ed. 2014).

35. Pieter van Dijk et al., THEORY AND PRACTICE OF THE EUROPEAN CONVENTION ON HUMAN RIGHTS 666 (Intersentia, 4th ed. 2006).

36. Mark W. Janis et al., EUROPEAN HUMAN RIGHTS LAW - TEXT AND MATERIALS 448 (Oxford Univ. Press, 3rd ed. 2008).

37. *Id*.

38. *Id*. at 449.

39. *Id*. at 448; Z v. Finland, App. No. 22009/93, 25 Eur. Ct. H.R. 371, ¶102 (1997).

40. Janis, *surpa* note 37, at 450; See v. City of Seattle, 387 U.S. 541 (1967).

41. Janis, *surpa* note 37, at 450.

42. *Id*. at 451.

43. *Id*.

44. *Id*. at 450.

45. *Id*.; See v. City of Seattle, 387 U.S. 541 (1967).

46. EUROPEAN CONVENTION ON HUMAN RIGHTS at art. 8.

47. Christoph Grabenwarter, EUROPÄISCHE MENSCHENRECHTSKONVENTION 194 (C.H. Beck, 3rd ed. 2008).

for, storing, or working with personal data.[48] While the ECHR addresses the state, the state has an obligation to take positive action to protect against human rights violations by non-state actors. Although the text of Article 8 ECHR refers to "private life",[49] the norm is understood to include business information as well.[50] The same norm protects communication: "the individual communication with others is part of the private sphere."[51] Article 8 ECHR also protects correspondence *expressis verbis*, which is understood to include phone and email as well.[52] The protection offered by Article 8 ECHR also covers the transfer of information in the context of legal proceedings.[53]

III. DOES SPYING CONSTITUTE "JURISDICTION" WITHIN THE MEANING OF ARTICLE 1 OF THE ECHR?

But does espionage constitute the jurisdiction, which is required by Article 1 ECHR in order to trigger the responsibility of states, under the Convention? States can be held accountable under the ECHR for acts which affect those outside their borders.[54] But not every state action leads to the victim falling under the jurisdiction of the state. Indeed, Article 1 ECHR requires at least some level of "authority and control over a person[.]"[55] In the case of hacking, this threshold will not be passed. But does this mean that victims will have no recourse under the Convention in such cases?

IV. DO STATES HAVE A POSITIVE OBLIGATION TO PROTECT RESIDENTS AGAINST FOREIGN CYBER ESPIONAGE?

In principle, states are not accountable for acts by other states that have effects within their territory.[56] But a state which is thus affected "still is under a positive obligation according to Article 1 [of the ECHR] to take diplomatic, economic, judicial and other measures that [a]re in its power to take and [which a]re in accordance with international law to secure […] the rights guaranteed by the Convention."[57]

Under the European Convention on Human Rights, states are not only obliged to refrain from harming holders of human rights, be they

48. *Id.*
49. EUROPEAN CONVENTION ON HUMAN RIGHTS at art. 8, §1.
50. Grabenwarter, *supra* note 47, at 195.
51. *Id.*
52. *Id.* at 198
53. Rainey, *supra* note 34, at 364.
54. Grabenwarter, *supra* note 11, at 7.
55. *Id.* at 8.
56. *Id.* at 7.
57. *Id.*

individuals or corporations,[58] but states also can be obliged to take positive steps in order to protect human rights. In the context of European Human Rights law, this duty is particularly relevant in the context of the right to private life.[59] Indeed, the distinction between positive and negative obligations under the right to private life seems to be minute[60] and the European Court of Human Rights appears to employ a "fair balance"[61] test[62] to weigh "the interests of the community and the interests of the individual"[63] against each other. In doing so, the Court will take the legitimate goals into account which are also included in paragraph 2 of Article 8 ECHR.[64] Just like states are obliged to take measures, such as the establishment of criminal law rules, the provision of effective law enforcement and the like, to protect your right to life against would be murderers. This positive dimension can also force states to take measures aimed at protecting their residents against human rights violations by other states. In the case of the Internet, though, this is hardly possible.

D. CONCLUDING REMARKS

In principle, espionage is legal under international law as far as the relations between states are concerned.[65] The same cannot be said of states' attempts to gain access to personal data under international human rights law. Information, which used to be accessible to outsiders only through state-run espionage, is now often the object of international communication.[66] As such, it can be accessed and abused. Perfect protection against foreign interference would require a closed national net. Closed national nets are incompatible with the spirit of the Internet and with fundamental human rights. Maximum protection would therefore require a major human rights violation. Online communication goes in both directions and users will have to play their part in protecting themselves. In a sense, the virtual world is not much different from real life; when walking down a crowded city street, one also exercises common sense in terms of personal security in order to protect oneself against *e.g.* robbery.

---

58. *Id.* at 3.
59. Rainey, *supra* note 34, at 365.
60. *Id.*
61. *Id.*
62. Dickson v. U.K., App. No. 44362/04, 2007-V Eur. Ct. H.R. 1, ¶71 (2007).
63. Rainey, *supra* note 34, at 365.
64. *Id.*
65. Philip Kunig, VÖLKERRECHT UND STAATLICHES RECHT 81-156, 143 (Wolfgang Graf Vizthum, 4th ed. 2007).
66. Stephan Hobe & Otto Kimminich, EINFÜHRUNG IN DAS VÖLKERRECHT 357 (A. Francke ed., 8th ed. 2004).

While the state can take some measures which make crimes less likely, it cannot prevent all crimes. The same applies to crimes committed online. Likewise, the responsibility for the crime rests with the perpetrator, not with the victim. While it is necessary to exercise caution online as well as offline, it is the perpetrator who has to be brought to justice for crimes that are committed with the use of the Internet in order to ensure a certain deterrent effect. This is what European Human Rights law can provide. The European Convention on Human Rights imposes obligations on states that aim to protect the human rights of Internet users. This framework, however, does not provide absolute protection. In so far as it becomes clear that both international law as well as the legal rules governing cyberspace remain incomplete. The ECHR at least offers a solid foundation on which state obligations can be established that will ultimately serve to ensure the protection not only of privacy but also of communication rights, all of which are protected under Article 8 ECHR.

Assuming that North Korea was indeed behind the attack against Sony, there are a number of serious implications. A company's capability to work within the legal frameworks applicable to it is parallel to the sovereignty of a state within the framework of international law. North Korea's actions have not only affected Sony negatively but if Sony were a country, this hacking attack would have been the equivalent of an act of war. In a world where every laptop is a weapon and in which major corporations have global reach and interests, the conflict between North Korea and Sony might simply be a new form of conflict. Like non-international armed conflicts before, this new type of conflict will also require some form of international legal regulation. Transnational corporations can play a role in creating international law.[67] It will be necessary to create a new subset of rules of International (Humanitarian) Law dealing with cyber conflicts between states and non-state actors. While this kind of conflict was until recently seen primarily as a conflict between states and non-state hackers (which could be regulated through national law and some international law elements, such as cooperation in law enforcement), recent developments show that a more comprehensive approach is necessary to provide an adequate legal reaction to state-hackers.

67. Stefan Kirchner, *TRANSNATIONALE UNTERNEHMEN ALS OBJEKTE UND SUBJEKTE DES VÖLKERRECHTS - ZWISCHEN VERANTWORTUNG UND TEILHABE* 219 (Jelena Bäumler et al. eds., 2010).