**International Journal of Communications Law & Policy**

Issue 9 - Special Issue on Cybercrime, Autumn 2004

# TRANSBORDER SEARCH: A NEW PERSPECTIVE IN LAW ENFORCEMENT?

*By Dr. Nicolai Seitz*[†]

**ABSTRACT**

Think about the following situation: you are a German police officer investigating a serious crime. Your suspect is an American citizen using a Yahoo-e-mail-account to communicate with his criminal partners. Now you are informed that critical evidence (an e-mail) was sent to the suspect's e-mail-account and is currently stored on Yahoo´s e-mail-server in New York. It is Sunday morning and there are indications that the e-mail will be deleted by the suspect in a few hours. Traditional methods of gaining access to the vital evidence, like letters rogatory, might take too long. What do you do? Is it permissible for you as a German police officer to hack the suspect's e-mail-account and to download the incriminating e-mail from the server located in New York?

This Article tries to find an answer to the question of when such a "transborder search" is currently admissible under public international law. It analyses the first (at least publicly known) criminal case worldwide in which a law enforcement agency (the United States Federal Bureau of Investigation) used this method to access and download evidence stored on server in a foreign country. After analysing the current legal situation the author comes to the conclusion that up to now a transborder search to access protected data is in principle inadmissible. However, there is an exception when the data are stored in the United States and extraordinary circumstances prevail. Therefore, the author's answer regarding the question above is "yes".

## I. TRANSBORDER SEARCH AND THE GORSHKOV-IVANOV CASE

The Internet confronts prosecuting authorities with new tasks and opportunities. In transnational prosecutions, it is more and more frequently the case that the relevant data for local preliminary investigations and criminal proceedings are stored on foreign servers. As a result, national prosecuting authorities are initially barred from direct physical access to these data.[1] The common slogan of the "unlimited Internet" conceals a significant problem confronting prosecuting authorities; thus far, there have only been rudimentary attempts at



[†] Ph.D. in Law (*Dr. iur.*) (University of Cologne); currently working for the Regional Court of Cologne; contact: Nicolai.Seitz@web.de. The author wishes to thank Boris Rotenberg for his kind assistance.

[1] In 80% of all German cases in which the Internet plays a role in committing or carrying out an offense, access to data located abroad is necessary for the criminal investigations. *See* BUNDESJUSTIZMINISTERIUM/ BUNDESINNENMINISTERIUM [GERMANY'S FEDERAL DEPARTMENT FOR LEGAL AFFAIRS/GERMANY'S FEDERAL DEPARTMENT FOR DOMESTIC AFFAIRS], PERIODISCHER SICHERHEITSBERICHT 2001 [Periodical security report 2001] at 204 (2001), *available at* http://www.bmi.bund.de/dokumente/Artikel/ix_49371.htm (last visited Feb. 20, 2004). Similar statistics for arbitrary Internet research are also mentioned by Germany's Federal Commissioner for Data Protection, BUNDESDATENSCHUTZBEAUFTRAGTER [FEDERAL COMMISSIONER FOR DATA PROTECTION], *18* TÄTIGKEITSBERICHT [18th ACTIVITY REPORT] 105, *available at* http://www.bfd.bund.de/information/18tb9900.pdf (83%) (last visited Feb. 20, 2004), as well as by Germany's Federal Criminal Investigation Agency, BUNDESKRIMINALAMT [FEDERAL CRIMINAL INVESTIGATION AGENCY], BEKÄMPFUNG DER KRIMINALITÄT IM INTERNET [CRIME COMBAT ON THE INTERNET] 151 (2000) (citing 80%). Thus, crossing national borders during the prosecution of Internet crime is no longer the exception, but the rule.

adequately resolving this difficulty.[2] An illustrative example of the problems associated with transnational prosecution of offenses on the Internet is a case which has recently been heard in the United States and which serves as the starting point for this essay: the Gorshkov-Ivanov case. The circumstances of the case were the following.

Around the end of 1999, certain unauthorized persons abused the Internet to hack into the networks of twenty United States businesses, including banks, credit card institutions, and Internet service providers. The unknown offenders gained access to credit card numbers and other information about financial transactions and used these to commit fraud. In February 2000, one of the affected firms, a credit report agency, received an e-mail stating that the e-mail sender had uncovered the "root password" which would give him unrestricted access to the firm's network. The e-mail sender threatened to delete all data from all computers connected to the network unless the firm hired him as a security consultant. The Federal Bureau of Investigation ("FBI"), which had been called upon to investigate, detected that the e-mail had been sent from an e-mail account provided by a Washington-based e-mail service provider whose network the offenders had also infiltrated. It turned out that the offenders had used two computers located in Chelyabinsk (Russia). The owners of the two computers were the Russian citizens Ivanov and Gorshkov. The FBI subsequently initiated an operation, code-named "Flyhook" and, in June 2000, established a pseudo-firm named "Invita" ostensibly specializing in security consultation for Internet firms. Invita offered jobs to both of the suspects, but demanded proof of their qualifications. To demonstrate their abilities, they were asked to hack into a firm website specifically created for this purpose. On November 10, 2000, the two suspects flew to Seattle, where FBI officers posing as employees of the firm provided computers on which specific recording programs ("sniffer programs") had been installed. With the computers, the suspects accessed their servers in Russia over the Internet, in order to retrieve the locally stored software which they needed for the demonstration. The passwords they used to access the servers in Russia were being recorded by the sniffer program. Ivanov and Gorshkov were arrested on the same day. Afraid that relevant data might be deleted in Russia, FBI officers accessed the Russian servers via the Internet using the obtained passwords. They downloaded 250 gigabytes of data, including stolen credit card numbers and other evidence. The two Russians were charged with multiple misdemeanors**,** and with the help of the data downloaded from Russia, they have already been convicted to fines and prison sentences. [3]

---

[2] *See* Peter Dieterle et al., [*Information Warfare*], KRIMINALISTIK 2003, 330, 336: "[The prosecution as a task within the sole responsibility of a nation state fails very quickly when its competences are confronted with the boundlessness of the Internet.]" For a more general view, see B. Scheffler, *in* WOLFGANG KILIAN & BENNO HEUSSEN, COMPUTERRECHTSHANDBUCH [COMPUTER LAW MANUAL] § 104 n.1 and Max-Peter Ratzel & Peter Beismann, *Der elektronische Handel im Internet* [The Electronic Commerce on the Internet], KRIMINALISTIK 2003, 642, 651 ("[National competences regulating legal matters face restrictions in the age of worldwide communication networks.]").

[3] *See* United States v. Ivanov, 175 F. Supp. 2d 367 (D. Conn. 2001); United States v. Gorshkov, 2001 WL 1024026 (W.D. Wash. 2001); Brendan I. Koerner, *From Russia with LoPHT*, LEGAL AFFAIRS, May-June 2002, at 35-38, *available at* http://www.legalaffairs.org/issues/May-June2002/feature_koerner_mayjun2002.html; Press Release, United States Department of Justice, Russian National Arrested and Indicted For Penetrating U.S. Corporate Computer Networks, Stealing Credit Card Numbers, and Extorting the Companies By Threatening to Damage Their Computers (May 7, 2001), *available at* http://www.usdoj.gov/criminal/cybercrime/ivanovIndict.htm (last visited Sept. 13, 2004); Press Release, United States Department of Justice, Russian Computer Hacker Indicted In California For Breaking Into Computer Systems And Extorting Victim Companies (June 20, 2001), *available at* http://www.usdoj.gov/criminal/cybercrime/ivanovIndict2.htm (last visited Sept. 2004); Press Release, United States Department of Justice, Russian National Indicted On Computer Intrusion Charges (August 16, 2001), *available at* http://www.usdoj.gov/ criminal/cybercrime/ivanovIndict3.htm (last visited Sept. 13, 2004); Press Release, United States Department of Justice, Russian Computer Hacker Convicted by Jury (October 10, 2001), *available at* http://www.usdoj.gov/criminal/cybercrime/gorshkovconvict.htm (last visited Sept 13, 2004). *See also* UNITED STATES DEPARTMENT OF JUSTICE, SEARCHING AND SEIZING COMPUTERS

At first glance, the case appears to be of little legal significance. Because of the FBI's creative course of action, the offenders could be identified, arrested and convicted by a United States court. Why, then, does the case acquire legal significance for prosecution authorities outside of the United States and why is it consequently worthy of closer examination?

The response is: The case is noteworthy because this is apparently the first case, worldwide, for whose prosecution the responsible authorities have employed a "transborder search" and in which the evidence obtained by means of this measure provided the basis of the conviction. A transborder search is defined as a search in which the Internet offers the opportunity to take unilateral measures to access data which are stored on servers in third countries, and in which agents of the state affected by the offense access the data without asking permission of the state (*i.e.*, by way of a letters rogatory) in which the data are stored. In the Gorshkov-Ivanov case, for example, the investigating officers directly accessed the offenders' servers in Russia from the United States instead of addressing a letters rogatory to the Russian authorities. The legal permissibility of such unilateral measures, used to access data stored on foreign networked servers from within the affected country, is at the moment increasingly discussed both nationally and internationally from the perspective of international law under the keywords "transborder search" and "transnational search".

The decisive legal question posed by transborder searches is whether a violation of the international principle of territoriality is caused by the access to the data stored on networked computers outside national territory, and if yes, whether this violation might under certain circumstances be justified.[4] The principle of territoriality in international law (alternatively also called the principle of formal territoriality)[5] categorically forbids a state to undertake a government act on foreign territory. Access via the Internet (or, in some cases, also via intranet) to data located on servers abroad could be held to be a violation of this principle (for more details, see Part II, *infra*).[6] As a general rule of international law,[7] the principle of territoriality is globally recognized and to be respected. Thus, if a transborder search qualifies as an infringement of the principle of territoriality, the course of action undertaken by the prosecuting authorities would be improper and, in case of a violation, would possibly render inadmissible evidence thus gained.[8]

---

AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 4 (2002) [hereinafter SEARCHING & SEIZING], *available at* http://www.usdoj.gov/criminal/ cybercrime/s&smanual2002.pdf (last visited Feb. 20, 2004) (discussing Gorshkov-Ivanov cases, albeit not with regards to the problem of the permissibility of transborder searches).

[4] For principle of territoriality, see KNUT IPSEN, VÖLKERRECHT [INTERNATIONAL LAW] § 23 nn.6-10 (4th ed. 1999) (providing additional bibliographic references); Karl-Friedrich Nadler, *Beweisaufnahme im Ausland* [*Hearing of Evidence Abroad*], Freibug i.Br. 1988, 18.

[5] *See* Rainer Spatscheck, *Steuerhinterziehung im Internet* [*Tax Evasion on the Internet*], StraFo 2000, 1, n.28 (providing further bibliographic references).

[6] It is, however, not a case of transborder search if prosecuting authorities find a networked computer which is currently displaying data that is normally stored abroad. The displayed data is then saved in the interim memory of the computer and therefore on domestic territory. It is a transborder search, however, if further data, which had not been in the interim memory, is retrieved. Regarding this matter, also compare ULRICH SIEBER, LEGAL ASPECTS OF COMPUTER-RELATED CRIME IN THE INFORMATION SOCIETY – COMCRIME-STUDY 107, n.239, *available at* http://europa.eu.int/InternetServiceProvider/legal/en/comcrime/sieber.doc (last visited Feb. 20, 2004); Ulrich Sieber, *Collecting and Using Evidence in the Field of Information Technology, in* ALBIN ESER & JONATAN THORMUNDSSON, OLD WAYS AND NEW NEEDS IN CRIMINAL LEGISLATION 203, n.25. Sieber suggests that this situation may be a possible permissible exception from the prohibition of transborder searches. Strictly speaking, however, this is not a case of transborder search, as the data is located domestically.

[7] *See* BVerfGE E 63, 343 (361, 373-74); Streinz, *in* MICHAEL SACHS, GRUNDGESETZ [BASIC LAW] Art. 25, n.51(f) (3d ed. 2003).

[8] For German law, see, e.g., WOLFGANG BÄR, DER ZUGRIFF AUF COMPUTERDATEN IM STRAFVERFAHREN [ACCESS TO COMPUTER DATA IN CRIMINAL PROCEEDINGS] 236; Rainer Spatschek & Jörg Alvermann, *Steuerfahndung ohne Grenzen? Auslandsermittlungen im Steuer- und Steuerstrafverfahren* [Tax Investigations

Answering the question of the permissibility of transborder search is also significant because letters rogatories, a traditional instrument of transnational cooperation, are often ineffective in investigations relating to the Internet. The disadvantage of letters rogatories is the long processing time (an average of one year in the case of Italy, and even two years in the case of Spain).[9] This is in conformity with data indicating that international jurisdiction takes an average of two years to backtrack the digital traces left by the offender during his/her offense on the Internet.[10] For investigations involving the Internet, the time factor plays a decisive role for several reasons. Many countries, such as Germany, have recently introduced data protection provisions under which data relevant as evidence (such as IP addresses) must be deleted after a certain period of time. Moreover, punishable contents are often made accessible on the Internet only for a short period of time, after which they are deleted. Furthermore, as the time span increases, there is a growing risk of the offender finding out about the investigations against him and benefiting from the ease with which data of evidentiary value may be deleted.[11] Finally, it has also occurred in the past that letters rogatories received no answer at all.[12] Traditional letters rogatories are, therefore, hardly promising for Internet-related investigations.[13]

Criminals have long known of these advantages and exploited them for their own purposes. Hackers, for example, often use several networked intermediary systems when intruding into foreign networked systems in order to complicate the detection of the original computer used. If the intermediary systems include computers located in Italy or Spain, the probability of obtaining relevant data without delay tends toward zero. According to German prosecuting authorities, offenders also relocate pornographic material to countries in which said material is not prohibited, and therefore systematically take advantage of divergences in global criminal legislation.[14]

In the past, various transnational institutions and organizations have made efforts to improve international cooperation with respect to these difficulties, and the first successful

---

Without Borders? Foreign Investigations and Criminal Fiscal Proceedings], IStR 2001, 33, 36; Spatscheck, *supra* note 6, at 7; Annette Marberth-Kubicki, *Internet und Strafrecht* [*Internet and Criminal Law*], StraFo 2002, 277, 281.

[9] *Cf.* Rainer Spatscheck & Jörg Spatscheck, *Beschlagnahme und Auswertung von verschlüsselten Computerdaten* [*Seizure and Survey of Encrypted Computer Data*], PStR 2000, 188, 190.

[10] *See* Krempl, *Polizeichef: Internet-Anbieter müssen Kundendaten länger speichern* [*Chief Police Officer: Internet Service Firms Must Save Client Data for a Longer Period of Time*], *in* HEISE ONLINE (Aug. 13, 2001), *at* http://www.heisenews.de/newsticker/data/jk-13.08.01-000/ (last visited Feb. 20, 2004).

[11] *See, e.g.*, BÄR, supra note 9, at 41 (describing a Swiss case handled by the Public Prosecutor's office in Frankfurt am Main, file no. 92 Js 34528/87, dated 1987. A firm (or, respectively, the senior employees) from Frankfurt was suspected of having committed investment fraud. A search of its premises only led to the discovery of a computer terminal without its own storage device, which was connected to the public telephone network. The business data was only retrievable by data telecommunication transfer and was stored on a central processor in Switzerland. Access via data telecommunication transfer was not undertaken by the prosecuting authorities (for unknown reasons). The headquarters of the firm in Monaco had the same access rights as the firm subsidiary in Frankfurt/Main and initiated the deletion of evidence while a letters rogatory by German authorities was handled in Switzerland. However, during a later search subject to the letters rogatory, authorities were able to confiscate backup copies of the relevant data.).

[12] *See* Frank Gehde, *Verfolgung von Straftaten im Internet* [*Persecution of Criminal Offences on the Internet*], DuD 2003, 496 , 499.

[13] *See* Jürgen P. Graf, *Internet: Straftaten und Strafverfolgung* [*Internet: Criminal Offences and Criminal Persecution*], DRiZ 1999, 281, 286; *see also* Hauke Scheffler & Christian Dressler, *Die Insuffizienz des Computerstrafrechts* [*The Insufficiency of Computer Criminal Law*], ZRP 2000, 514 (discussing from a critical point of view).

[14] *Cf.* Peter Wiedemann, *Tatwerkzeug Internet* [*Criminal Instrument Internet*], KRIMINALISTIK 2000, 229.

results can be seen. The Convention on Cybercrime of the Council of Europe,[15] for example, envisages in Article 35 the establishment of a 24/7-point of contact which will process letters rogatories around the clock (24 hours, 7 days a week). Nevertheless, the involvement of a third country to undertake the desired measure causes time delays which may, in certain cases, thwart investigatory success or which can make these appear unacceptable for other reasons.[16] The only remaining option, then, is to conduct a transborder search.

## II. LEGAL PERMISSIBILITY OF "TRANSBORDER SEARCHES"

The investigating officers in the Gorshkov-Ivanov case had decided to take this course of action. In the court trials against the two offenders, however, the question of whether the officers' approach was permissible according to international law was not addressed. Even the manual about electronic evidence distributed by the United States Department of Justice ("USDOJ"), which also attends to the implications of a transborder search with respect to (international) law, does not discuss the Gorshkov-Ivanov case (in this context).[17] The fact that the computers on which the relevant data were stored were located in Russia and not in

[15] Convention on Cybercrime, *opened for* signature Nov. 23, 2001, *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (last visited Feb. 20, 2004). The convention has so far been ratified by three countries (Albania, Croatia and Estonia). Ratification by the United States is still outstanding. President Bush has recently asked the Senate to consent to the Convention. Press Release, The White House, Message to the Senate of the United States (Nov. 17, 2003) *available at* http://www.whitehouse.gov/news/ releases/2003/11/20031117-11.html (last visited Feb. 20, 2004) (announcing therein that the United States had actively participated in the establishment of the Convention by observation and signed the Convention on Nov. 23, 2001). The letter further states that the Convention could be an effective tool to fight cybercrime such as identity theft and child pornography globally. The ratification of the Convention would remove barriers on the way toward international cooperation. As a result, according to President Bush, it could become more difficult for criminal offenders to retreat to safe places from which to cause damage to the United States.

[16] A good example of this is given by Michael A. Sussmann in his article, *The Critical Challenges From International High-Tech and Computer-related Crime at the Millennium*:

> "A hacker, going on-line through the Internet, breaks into computers that the Federal Aviation Administration (FAA) uses for air traffic control. He disrupts a regional air traffic network, and the disruption causes the crash of a DC-10 in the Rocky Mountains, killing all aboard. The FAA and the FBI know there has been a hacker intrusion, originating through the Internet, but nothing else. Since anyone can access the Internet from anywhere in the world, the FBI has no idea where the hacker may be located. Moreover, they do not know the motive of the attack or the identity of the attackers. Is it a terrorist group, targeting the United States and likely to strike again at any time, or is it a fourteen-year-old hacker whose prank has spun tragically out of control? Within thirty minutes of the plane crash, the FBI tracks the source of the attack to an Internet Service Provider (ISP) in Germany. Assuming the worst, another attack could occur at any time, and hundreds of planes in flight over the United States are at risk. The next investigative step is to determine whether the ISP in Germany is a mere conduit, or whether the attack actually originated with a subscriber to that service. In either case, the FBI needs the assistance of the German ISP to help identify the source of the attack, but it is now 3:00 a.m. in Germany.
>
> Does the FBI dare wait until morning in Europe to seek formal legal assistance from Germany or permission from the German government to continue its investigation within their borders?

Michael A. Sussmann, *The Critical Challenges From International High-Tech and Computer-related Crime at the Millennium*, 9 DUKE J. OF COMP. & INT'L L. 451, 453-54 (1999). Similar difficulties also arise, for example, when a website is "split up", *i.e.*, the data of a website is not stored on a single server but, comparable to a mosaic, different parts of the website are stored on servers in various countries, see Scott Charney, *Wir wollen auch für andere Länder eine Führungsrolle einnehmen* [*We Also Want to Be a Guide For Other Countries*], interview by Christiane Schulzki-Haddouti, *available at* http://jya.com/g9-charney.htm (last visited Feb. 20, 2004).

[17] *See* USDOJ, SEARCHING & SEIZING, *supra* note 4, at 25. The defense lawyers in *Gorshkov* have not mentioned this point either. *See* Koerner, *supra* note 4, at 37.

the United States even had a negative effect on the accused. This was the case because a United States District Court held that the protection of the United States Constitution, which applied only within the United States and only to United States citizens, was not available to them.[18] The need to discuss legal permissibility, however, was already evident because Russia's Federal Secret Bureau (FSB), responsible for computer crimes, protested the FBI's course of action after the procedure had become known.[19] Since then, the FSB has even induced preliminary proceedings in Russia against the FBI officer leading the operation, charging him with illegal intrusion into computer systems.[20] According to an FSB spokesperson, the case is a matter of principle, as there is the danger that the FBI will continue to proceed this way in the future. However, the responsible court as well as the United States government refuses to allow the arrest of the FBI officer.[21]

To answer the question of the international legal permissibility of a transborder search, it is advisable to first differentiate whether the transborder search in the third country aims at the retrieval of generally accessible data or of data that are not freely accessible. The category of generally accessible data is comprised of all data which are not subject to any special pre-conditions. That includes, for example, access via a "guest account," which is open to everyone. The Gorshkov-Ivanov case, on the contrary, deals with not freely accessible data, because the data could only be accessed by password.

## A. Transborder Searches in the Case of Generally Accessible Data

In international literature (no jurisdiction exists so far), the permissibility of a transborder search with respect to generally accessible data is currently the subject of controversial discussion. In part, the compatibility of transborder searches in the case of generally accessible data with the international principle of territoriality is affirmed,[22] with strongly varying justifications given. The then-senior prosecutor at the Federal Court of Germany (BGH) and current judge at the same court, Jürgen Graf, for example, wants to allow transborder searches for reasons of practicability, based on his belief that a reliable conclusion about the location of the computer cannot be drawn by the Uniform Resource Locator (URL).[23] Behind this lies the assumption that, without a transborder search, an investigation on the Internet could not be conducted at all by the prosecuting authorities, because an infringement of the principle of territoriality could never be completely precluded.

---

[18] *See* United States v. Gorshkov, 2001 WL 1024026 (W.D. Wash. 2001).

[19] *See USA: Russischer Hacker muss drei Jahre in Haft* [USA: Russian Hacker Must Go to Prison For Three Years], *in* CHIP ONLINE, *at* http://www.chip.de/news_stories/news_stories_8863217.html (last visited Feb. 20, 2004). However, the Russian government has so far dispensed with a formal protest. *See* Koerner, *supra* note 4, at 38.

[20] *See FSB charges FBI with Hacking*, *in* RADIO FREE EUROPE/RADIO LIBERTY (Aug. 16, 2001), *at* http://www.rferl.org/newsline/2002/08/1-RUS/rus-160802.asp (last visited Feb. 20, 2004).

[21] *See id*, *supra* note 21. For his performance in this case, the leading FBI officer received an award. *See* FEDERAL BUREAU OF INVESTIGATION, AWARDS FOR OUTSTANDING CRIMINAL AND COUNTERTERRORISM INVESTIGATIONS (2002), *available at* http://www.fbi.gov/page2/seattle.htm (last visited Feb. 20, 2004).

[22] For an American point of view, see USDOJ, SEARCHING & SEIZING, *supra* note 4, at 25 ("There is general agreement that access to publicly available materials in Country A, such as those posted to a public Web site . . . are permissible without prior consultations"); For a German point of view, see Michael Germann, GEFAHRENABWEHR UND STRAFVERFOLGUNG IM INTERNET [HAZARD CONTROL AND CRIMINAL PERSECUTION ON THE INTERNET] 652 (1999); ROBERT JOFER, STRAFVERFOLGUNG IM INTERNET [PROSECUTION ON THE INTERNET] 196 (1996); Jürgen P. Graf, *Befugnisse und Grenzen der Ermittlungsbehörden* [*Powers and Boundaries of Prosecution Authorities*], DPolBl. 4/2001, 6, 9.

[23] *See* Graf, *supra* note 23, at 9.

Robert Jofer,[24] on the other hand, chooses a different approach. First of all, he declares the traditional concept for defining an infringement of the principle of territoriality to be unsuitable. The main argument in favor of a violation of international law is inapplicable because the officer undertaking the data retrieval is physically not in foreign territory. However, he uses technical means to activate a computer in foreign territory. The decisive criterion thus cannot be the place of the offense but only the intensity with which the legal framework of the country from which the data are retrieved is affected. This, in turn, depends on whether an intrusion into the individual rights of a foreign citizen results from the retrieval of generally accessible data. With respect to the retrieval of generally accessible data, this is to be rejected because the officer does not undertake any acts of deception regarding his role as part of a prosecuting authority and, comparable to reading a foreign journal, merely takes advantage of an offer made to the public. By tolerating the Internet as an institution, the state has permitted data traffic in its national territory, traffic which includes the retrieval of data from abroad. Even with respect to external appearances, a retrieval of generally accessible data from abroad does not encroach upon the rights of a citizen; the measure is, rather, comparable to the video camera recording of illegal border crossings by the border police.

Michael Germann, too, reaches a similar conclusion, raising the question of whether the communication of the officer includes an aspect of national sovereignty.[25] The communication-based situation suggests a classification with respect to anonymity: if access is gained to public and anonymous (*i.e.*, generally accessible) Internet offerings, the person retrieving data does not arrogate sovereign power. No country would consider such an investigatory act an infringement of territorial sovereignty. If the latter circumstance were not to exclude an intrusion, the assumption of a justifying toleration should be valid. Finally, Harald Schaumburg notably goes still a step further with his view that foreign-oriented intelligence measures conducted from domestic territory are always permissible because a physical entry into foreign territory is not undertaken.[26]

The opposite view rejects the permissibility of the retrieval of data from foreign computers even in the case of generally accessible data.[27] According to this view, the principle of territoriality prohibits any form of sovereign activity by prosecuting authorities in foreign territory regardless of whether or not it is a measure which includes an intrusion.[28] The newly arisen possibilities of transfer resulting from networked systems, with which data processing can be initiated abroad, would, in the case of a transborder search, be used like an

---

[24] *See* JOFER, *supra* note 23, at 193.

[25] *See* GERMANN, *supra* note 23, at 651.

[26] *See* HARALD SCHAUMBURG, INTERNATIONALES STEUERRECHT [INTERNATIONAL FISCAL LAW] § 19.2 (2d ed. 1998) (referring to investigations in criminal tax proceedings). He mentions as evidence a ruling by the German Federal Financial Court in Germany, BStBl. III 1959, 181, which itself, however, does not exactly support his view. The Federal Financial Court states in its ruling that apart from the formal delivery abroad, the simplified form of delivery of formal official notifications and rulings by the post office, initiated by a domestic German authority, is also impermissible because of a violation of the principle of territoriality. In this way, the Federal Financial Court takes a stance exactly opposite to Schaumburg's view.

[27] *See* MARCO GERCKE, RECHTSWIDRIGE INHALTE IM INTERNET [ILLICIT CONTENTS ON THE INTERNET] 171 (2000); Ulrich Sieber, *in* THOMAS HOEREN & ULRICH SIEBER, HANDBUCH MULTIMEDIARECHT [HANDBOOK MULTIMEDIA LAW] § 19, n.736 (2004). The Bundestag, the German Federal Parliament, also argues in this direction. *See* BT-Drs. 13/11002, 117 (stating "[Due to the principle of territoriality this [an access to stored data] is as a rule to be avoided, at any case if the server is located abroad.]"). The Bundestag does not, however, differentiate between generally accessible and not freely accessible data. An opposite view without a differentiation between generally accessible and generally non-accessible data is presented by Rainer Spatscheck. *See* Spatscheck, *supra* note 6, at 7. *See also* IRINI E. VASSILAKI, MATERIELLES STRAFRECHT, STRAFPROZESSRECHT, RECHTSINFORMATIK UND INFORMATIONSGESELLSCHAFT [CRIMINAL LAW, CRIMINAL PROCEDURAL LAW, COMPUTER SCIENCE LAW AND INFORMATION SOCIETY] 347, 355 (2002), *at* http://www.alfred-buellesbach.de/PDF/33_Vassilaki_Materielles.pdf (last visited Feb. 20, 2004).

[28] *See* GERCKE, *supra* note 28 at 171. *See also* Sieber, *supra* note 28, § 19, n.736.

"extended arm" by the prosecuting authorities, and the intensity of intrusion is comparable to that of physical presence in the territory.[29] The right of a state to decide autonomously whether or not investigations shall be undertaken in its sovereign territory must not be circumvented with the help of advanced communications technologies.[30] It should be noted that a particular hazard results from the quantity of data which can be obtained unnoticed. A retrieval of generally accessible data does not lead to an infringement of private interests. However, because the data retrieval contributes to the execution of a nationally sovereign act, national sovereign interests are, in the end, also involved.

When considering the problem from a dogmatic perspective, the solution can be reached by answering two questions: Is the principle of territoriality affected by the retrieval of generally accessible data, and if so, does international law permit such a measure? The literature precisely emphasizes a particular characteristic of transborder searches that is relevant to the first question, namely that the physical presence of the civil servant representing a foreign country's sovereign power on the territory of the third country is, unlike in a usual investigation, not essential. In this respect, the comparison to the monitoring of foreign territory from a domestic position suggests itself (for example, by border police officers to uncover illegal boundary crossings or by intelligence satellites). According to conventional wisdom, such monitoring does not violate the international principle of territoriality.[31] A closer inspection shows, however, that the measures are not comparable. Unlike the comparison case, a transborder search brings about physically perceptible changes to the outside world in the territory of the third country because data processing is initiated on servers that are located in the foreign state. The measure is not restricted, as in the example of border protection, to pure monitoring of activities occurring in foreign territory, but in fact initiates new processes. Thereby it cannot make a difference whether the acting officer is physically present at the foreign site of the server when undertaking the measure, or whether he accesses the server over the Internet or in some cases also over an intranet. The result of his activity is the same in both cases: data processing is initiated on servers which are located in foreign sovereign territory. The decisive criterion to answer the question whether or not a violation of the principle of territoriality occurs is thereafter not the physical presence in foreign sovereign territory but whether the measure causally precipitates a perceptible change in the outside world in foreign territory.

The principle of territoriality, including the sole right of each country to decide whether or not criminal investigations may be undertaken in its territory, must not be annulled by novel communication medias such as the Internet. In a transborder search, the executing officer thus does not only act domestically, but also abroad.[32] The principle of territoriality is thereby affected by the execution of a transborder search, and the question remains open whether the resulting infringement of national sovereignty is justified in international law.

With respect to dogmatics, such a justification can exclusively be derived from recognized legal sources of international law. As legal sources of international law, international accords (treaties), international customary law (practice in law of nations) as well as recognized general legal principles are to be named.[33] The reasons of practicability

[29] *See* BÄR, *supra* note 9, at 235. *See also* Wolfgang Bär *in* HEINZ-BERNHARD WABNITZ & THOMAS JANOVSKY, HANDBUCH DES WIRTSCHAFTS- UND STEUERSTRAFRECHTS [HANDBOOK OF ECONOMIC AND FISCAL CRIMINAL LAW] § 25 n.23 (2d ed. 2004).
[30] *See* Spatscheck, *supra* note 6, at 7.
[31] *See* Wolfgang Graf Vitzhum, *in* WOLFGANG GRAF VITZHUM, VÖLKERRECHT [INTERNATIONAL LAW] § 1 n.139 (5th ed. 1997).
[32] In this respect, the physical presence is replaced by a "virtual presence". *See* Wolfgang Kuner, *Internationale Zuständigkeitskonflikte im Internet* [*International Jurisdictional Conflicts on the Internet*], CR 1996, 453, 454 (in another context).
[33] *See* IPSEN, *supra* note 5, §3 n.3; Art. 38 I Statute of the International Court of Justice.

brought forth in the literature are, accordingly, not a sustainable basis for justification, nor are the various classifications of public and anonymous communication or of the intensity of encroachment on the legal framework of the affected country. Such differentiations are not based on any of the recognized legal sources.

The problem of transborder searches has already been discussed internationally. As early as 1995, the Council of Europe engaged with the topic of transborder searches within the framework of a study titled *Concerning Problems of Criminal Procedural Law Connected with Information Technology*.[34] The Council of Europe then recommended that access to internationally stored data by way of networks be permitted in case immediate action is necessary.[35] The study became a topical issue again on the occasion of the preparations for the Convention on Cybercrime, and the recommendation was taken into consideration in Article 32 of the Convention on Cybercrime.

Article 32 of the Convention on Cybercrime, which has thus far been ratified by thirty-three states, constitutes the first agreement in international law which attends to the question of transborder searches. According to Article 32 (a) of the Convention on Cybercrime, a state may retrieve generally accessible data independently of the geographical location of their storage unit without having to ask for the consent of any other state.[36] A transborder search with respect to generally accessible data is, as a result, explicitly permitted.

However, even without the existence of Article 32 (a) of the Convention on Cybercrime, the retrieval of generally accessible data is recognized as part of international customary law. A pre-condition for the development of customary law is that a behavior be practiced over a certain period of time and be considered justifiable by all involved parties.[37] The examination of data in generally accessible Internet sources within the framework of a sovereign activity has been and is practiced daily, without states taking offense at this practice.[38] This implies that this practice has been tacitly tolerated and is considered lawful. In

---

[34] Council of Europe, Recommendation No. R (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedure Law Connected with Information Technology (adopted Sept. 11, 1995*), available* at http://www.usdoj.gov/criminal/cybercrime/crycoe.htm (last visited Sept. 20, 2004).

[35] Council of Europe, *supra* note 35, Appendix § VII (17):

> The power to extend a search to other computer systems should also be applicable when the system is located in a foreign jurisdiction, provided that immediate action is required. In order to avoid possible violations of state sovereignty or international law, an unambiguous legal basis for such extended search and seizure should be established. Therefore, there is an urgent need for negotiating international agreements as to how, when and to what extent such search and seizure should be permitted.

[36] Article 32 (a) of the Convention reads "A Party may, without the authorization of another Party, (a) access publicly available (open source) stored computer data, regardless of where the data is located geographically." Convention on Cybercrime, *opened for* signature Nov. 23, 2001, *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (last visited Feb. 20, 2004).

[37] KARL DOEHRING, VÖLKERRECHT [INTERNATIONAL LAW] § 4 n.286 (1999).

[38] *E.g.*, in non-specified Internet investigations by the German Federal Criminal Office. S*ee* Wolfgang Bär, *Strafverfahrensrechtliche Aspekte der Online-Kommunikation* [*Criminal Procedural Aspects of Online-Communication*], *in* DETLEF KRÖGER & MARC A. GIMMY, HANDBUCH ZUM INTERNET [INTERNET HANDBOOK] 637 (2d ed. 2002); BUNDESBEAUFTRAGTER FÜR DEN DATENSCHUTZ, *supra* note 1, at 105; *Straftaten im Internet - BKA sucht illegale Netzinhalte* [*Offenses on the Internet – The BKA Searches For Illegal Internet Content*], CHIP ONLINE, *at* http://www.chip.de/news_stories/news_stories_8934703.html (last visited Feb. 20, 2004). Switzerland also undertakes non-specified Internet investigations to prosecute offenses. S*ee* Nick Luethi, *Schweizer Cybercops nehmen Dienst wieder auf* [*Swiss Cyber Cops Are On Duty Again*], HEISE ONLINE, *at* http://www.heise.de/tp/deutsch/inhalt/te/13911/1.html (last visited Feb. 20, 2004); *Schweizer Polizei betreibt wieder Internet-Monitoring* [*Swiss police is again monitoring the Internet*], HEISE ONLINE (Jan. 7, 2003), *at* http://www.heise.de/newsticker/data/jk-07.01.03-001/ (last visited Feb. 20, 2004).

this respect, Article 32 (a) of the Convention on Cybercrime merely codifies the hitherto existing practice.

Therefore, as a first result, the following can be recorded: a transborder search is permissible as long as the access is to generally accessible data.

## B. Transborder Searches in the Case of Not Freely Accessible Data

However, generally available data are, as a rule, hardly fruitful for preliminary and criminal proceedings. Punishable contents or evidence are seldom made accessible on the Internet without an admission control mechanism. Consequently, it is more significant to answer the question whether access to not freely accessible (protected) data is also permissible. The comments in the literature with respect to this question are considerably more univocal than in the case of generally accessible data.

### *1. Prevalent View*

The strongly predominant view holds that a transborder search with respect to protected data is impermissible because of the resulting violation of the principle of territoriality if no explicit consent is expressed by the affected state.[39] The procedure violates existing agreements on legal assistance. Thus, in its 1995 recommendation, even the Council of Europe considers transborder searches to cause an infringement of international principles, because otherwise the demand[40] expressed there for the establishment of an unambiguous legal basis would have been superfluous.[41]

---

[39] *See* Rainer Spatscheck & Jörg Alvermann, *Internet-Ermittlungen im Steuerstrafprozess* [*Internet-Investigations in Criminal Fiscal Proceedings*], wistra 1999, 333, 334; Spatscheck, *supra* note 6, at 7; Manfred Möhrenschläger, *Internationale Regelungen durch die „Cyber-Crime"-Konvention des Europarates* [*International Provisions in the "Cyber-Crime"-Convention of the Council of Europe*], *in* JÜRGEN WELP, KRIMINALITÄT@NET [CRIME@NET] 97, 110 (2003); Kurt Ringel, *Rechtsprobleme beim Zugriff auf EDV-Beweismittel* [*Legal Problems Regarding Access to DP-Evidence*], DPolBl. 3/1998, 14, 17 (legal situation unspecified, "[but most states, including the Federal Republic of Germany, are likely to see a violation of their sovereignty in a transnational investigation that has not been permitted]"); Wolfgang Bär, *supra* note 30, § 25 n.23; Dieterle et al., *supra* note 2, at 337, 345; Hans-Werner Moritz, *Anmerkung zu AG München, Urt. v. 28.05.1998 – 8340 Ds 465 Js 173158/95* [*Remarks to AG München, Decision of 28.05.1998 – 8340 Ds 465 Js 173158/95*], CR 1998, 505, 509; Roland Derksen, *Perspektiven für eine wirksame Bekämpfung von Rechtsradikalis-mus und Rassismus im Internet* [*Perspectives for an Effective Combat Against Right Wing Radicalism and Racism on the Internet*], ZFIS 1999, 150, 155; THE COMPUTER RELATED CRIME RESEARCH UNIT, STUDY FOR EU: STUDY ON LEGAL ISSUES RELEVANT TO COMBATING CRIMINAL ACTIVITIES PERPETRATED THROUGH ELECTRONIC COMMERCE § 3 ("Recommendations") (2000), *at* http://europa.eu.int/InternetServiceProviderO/eif/InternetPoliciesSite/Crime/Study2000/Report.html (last visited Feb. 20, 2004); Gabriele Schmölzer, *Rechtliche Situation der Informationsregulierung* [*Legal Situation of Information Control*], *in* URSULA MAIER-RABLER ET AL., NETZ OHNE EIGENSCHAFTEN [NET WITHOUT CHARACTERISTICS; STUDY FOR THE AUSTRIAN FEDERAL MINISTRY OF SCIENCE AND RESEARCH] 52 (1995); Ulrich Sieber, *"Cyberlaw: Die Entwicklung im deutschen Recht"* [*"Cyberlaw': The Development in German Law*], *in* WILLIAM R. CHESWICK & STEVEN M. BELLOVIN, FIREWALLS UND SICHERHEIT IM INTERNET [FIREWALLS AND INTERNET SECURITY] 283, 303 (2d ed. 1995); Sieber, *Collecting & Using*, *supra* note 7, at 211-12; Sieber, *Legal Aspects*, *supra* note 7, at 106 ("[Particular problems regarding transnational measures. It is unclear in all countries, which have been examined, whether such activities infringe national sovereignty or not.]"). In part, however, without a differentiation between generally accessible data and not freely accessible data. As the then-Secretary of State in the German Department for Domestic Affairs and the current German Federal Minister of Justice stated in 2000, in an interview with Christiane Schulzki-Haddouti, a transborder search would "[affect the national sovereignty of our country and possibly the basic rights of individual citizens.]" Interview by Christiane Schulzki-Haddouti with Brigitte Zypries (2000). Whether or not the modification is considered permissible with respect to international law cannot, however, be concluded from the statement. *See also* Steffen Wettig, *Verantwortlichkeit im Netz - Wer haftet wofür?* [*Responsibility on the Net – Who is Liable For What?*], JurPC Web-Dok. 124/2003, ¶ 4, *at* http://www.jurpc.de/aufsatz/20030124.htm (Jürgen P. Graf, judge of the Federal Court of Germany, stating "[transnational investigations and online-searches and seizures are currently unthinkable.])" (last visited Feb. 20, 2004).

[40] *See* Council of Europe, *supra* note 35, Appendix § VII (17).

[41] Bär, *supra* note 39, at 651; Bär, *supra* note 30, § 25 n.25.

However, two modifications of this maxim are being discussed. First of all, an exception is considered for the case in which the person subject to the transborder search agrees to the data retrieval.[42] The majority of voices, however, reject such an exception, arguing that national sovereignty is not at the disposition of the individual.[43] Rather, the explicit consent of the responsible authority of the third country is needed to make a transborder search permissible in the case of protected data. [44]

The second exception is for so-called "good faith" cases, in which either the acting prosecuting authority erroneously assumed the data to be located in its own sovereign territory, or in which the location of a server was unclear or could not be identified with certainty.[45] One argument in favor of this is that otherwise the acting state would have to significantly renounce its executive power in its own sovereign territory.[46] An international obligation to refrain from state activity which could indirectly also have transnational effects restricts the territorial sovereignty of the acting country too much, because international law does not intend to reduce the exercise of state authority within a country. A use of foreign telecommunications systems cannot be excluded with certainty even for the case that both communicating partners are in the territory of a given country.

Wolfgang Bär, notably, goes even one step further.[47] While in his view, too, the principle of territoriality is violated, he nevertheless argues that the preliminary storage of data is always permissible in order to gain time to seek the affected state's permission to use the data in concrete criminal proceedings. Thus, even if prosecuting authorities know that the data are stored in another state, according to this view, access to these data and the subsequent preliminary storage is permissible until a decision has been reached by the affected country.

### *2. Opposite View*

The opposite view, which considers a transborder search permissible even for the case of not freely accessible data, is, in German literature, only supported by Olaf von Briehl and Dirk Ehlscheid.[48] In this view, provided that the data access by the prosecuting authorities does not go beyond that of the concerned permittee, the intensity of intrusion is so low, given the lack of the officer's physical presence on foreign territory, that the transborder search cannot be considered to be an infringement of foreign sovereignty. The two authors are supported especially in international literature, where the commencement of a transborder

---

[42] *See* USDOJ, SEARCHING & SEIZING, *supra* note 4, at 25 (stating "There is general agreement that . . . access to materials in Country A with the consent of the owner/custodian of those materials, are permissible without prior consultations."). In German literature, see Kurt Ringel, *supra* note 40, at 17.

[43] Moritz, *supra* note 40, at 509; Spatscheck, *supra* note 6, at 7; Spatscheck & Alvermann, *supra* note 39, at 334; Jens Gruhl, *"Grenzenlose" Ermittlungen im Internet?* [*"Boundless" Investigations on the Internet?*], *in* WELP, *supra* note 40, at 67, 73. For prosecuting measures generally, see KLAUS TIPKE & HEINRICH WILHELM KRUSE, ABGABENORDNUNG [FISCAL CODE] § 117 n.3 (2004); Spatschek & Alverman, *supra* note 9, at 33; SCHAUMBURG, *supra* note 27, §19.2.

[44] Spatscheck & Alvermann, *supra* note 40, at 334 (considering a transborder search impermissible, even if German investigating officers undertake an investigation when it is beknown to the other country, and they require an explicit consent of the responsible court of the third country at the least).

[45] *See* GERMANN, *supra* note 23], at 644, 654; COUNCIL OF EUROPE, CONVENTION ON CYBERCRIME EXPLANATORY REPORT n.191, *available at* http://conventions.coe.int/Treaty/EN/projets/FinalCyberRapex.htm (last visited Feb. 20, 2004); Ulrich Sieber, *Legal Aspects*, *supra* note 7, n.239; Sieber, *Collecting & Using*, *supra* note 7, n.25.

[46] *See* GERMANN, *supra* note 23, at 644, 654.

[47] *See* Bär, *supra* note 30, § 25 n.23.

[48] OLAF G. VON BRIEL & DIRK EHLSCHEID, STEUERSTRAFRECHT [CRIMINAL TAX LAW] 451-52 (2d ed. 2001); probably Sönke Hilbrans, *Verfassungskonflikte im Cyberspace* [*Constitutional Conflicts in Cyberspace*], Datenschutz Nachrichten 2/2001, 16, 18 (according to which "[the traditional concept of territorial sovereignty is no longer assumed in cyberspace.]").

search under certain pre-conditions is demanded in many instances.[49] Michael Sussmann, for example, considers a transborder search to be permissible in the existence of "exigent circumstances," such as acute danger to life.[50]

The views of Jack Goldsmith go in the same direction.[51] The starting point of his deliberation is the statement that technological changes, as they occur, alter the understanding of the normative significance of territorial sovereignty. In addition, the practice nowadays recognized by international law is that a nation may regulate activities in another nation if the activities in the third country cause local harm in the regulating country. An example of this is the regulation of foreign markets by United States antitrust legislation before World War II. This regulation was then considered, particularly by European states, to be an impermissible encroachment on their national sovereignty. Over the years a paradigm shift has taken place, and by now the regulation of foreign markets in connection with a domestic issue is considered internationally impermissible. International positions with respect to cybercrime have gone in a similar direction. In the case of a transnational cybercrime with a subsequent transborder search, a mutual violation of the principle of territoriality occurs, one committed by the state in which the criminal activity took place, and the other by the state in which damage was caused by the activity and which attempts to prevent this with the help of unilateral extraterritorial measures. The toleration and acquiescence, respectively, of damaging activity in a state's own territory is as much an infringement of sovereignty as the violated country's retrieval of the data created by the activity and relevant as evidence. Under special circumstances, a transborder search should therefore be permissible.

### *3. Own Perspective*

There are several problems with the argument in subpart B(2). First, it is impossible to speak of acquiescence to the criminal activities. Already, the existence of criminal laws such as § 202 of the German criminal code or § 271 of the Swiss criminal code, which declare the damaging action (*i.e.*, "hacking") to be liable to punishment, shows that states in which the damaging activity is initiated do not express toleration, but instead, disapprove of the behavior. Second, the damaging activity is furthermore conducted by private individuals, so that holding a state responsible for that behavior is at least difficult. A mutual violation of the international principle of territoriality is therefore almost unthinkable and cannot serve as a justification for transborder searches. Even if one were to construct a violation of international law by referring to "toleration," this tort does not inevitably legitimize further violation of international law.

---

[49] *See, e.g.*, COUNCIL OF EUROPE, GEMEINSAMER STANDPUNKT [COMMON POINT OF VIEW] 1 (May 27, 1999), Official Paper EG L 142 (June 5, 1999) (commenting on the negotiations in the Council of Europe about the agreement on cybercrime and allowing exceptional cases such as certain severe criminal offenses); ABRAHAM SOFAER ET AL., CENTER FOR INTERNATIONAL SECURITY AND COOPERATION, A PROPOSAL FOR AN INTERNATIONAL CONVENTION ON CYBER CRIME AND TERRORISM 14 *at* http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm (last visited Feb. 20, 2004). Article 6(5) of the proposal reads

> States Parties shall be free to engage in reasonable, electronic methods of investigation of conduct covered by Articles 3 and 4 of this Convention, over which they have jurisdiction to prosecute under Article 5, even if such conduct results in the transfer of electronic signals into the territory of other States Parties. A State Party aware that its investigative efforts will likely result in such transfers of electronic signals shall as soon as practicable inform all affected States Parties of such efforts.

[50] Sussmann, *supra* note 17, at 471 (giving a hypothetical involving air traffic).

[51] *See* Jack Goldsmith, *Cybercrime and Jurisdiction*, *at* http://www.oas.org/juridico/english/cybercrime_and_jurisdiction.htm (last visited Feb. 20, 2004).

The von Briel/Ehlscheid view, which holds that transborder searches are merely a low-intensity encroachment, is not convincing either. The existence of norms, expressed by statutes such as § 202 of the German criminal code or § 271 of the Swiss criminal code, which address transborder searches, already demonstrates that transborder searches are perceived to be an encroachment of high intensity. The de minimis level beneath which the von Briehl/Ehlscheid view would apparently like to locate transborder searches is certainly exceeded.

The standard for the international evaluation of transborder searches with respect to protected data must rather, as in the case of generally accessible data, be based on the question of whether the legal sources of international law permit such a measure. Should this be the case, then transborder searches do not circumvent letters rogatories, because then, following the will of the subjects of international law, agreements on legal assistance are to be considered and interpreted as subordinate to the disagreeing legal sources.

In again consulting Article 32 of the Convention on Cybercrime, one will notice that, in contrast to the question of access to generally accessible data, and contrary to the previous recommendation of the Council of Europe, the access to not freely accessible data remains unregulated. Article 32 (b) of the Convention on Cybercrime only establishes that, in the case that consent of the legally authorized person has been given, prosecuting authorities are permitted to access stored data.[52] This is remarkable because a legal definition of "authorized person" is neither given by the Convention on Cybercrime itself nor by the explanatory report. The explanatory report states, for example, that the authorized person must be defined according to the respective circumstances and the applicable law of each individual case.[53] One example given is a situation in which an e-mail service provider has saved a private e-mail in a state other than the state of origin. According to the justification given, the e-mail service provider could possibly be regarded as an authorized person in the sense of Article 32 (b) of the Convention because the storage abroad is a consequence of the provider's will.

The term "authorized persons" is consequently not restricted to the affected person from whom the data stem. It may include third persons if the storage abroad results from their will and not from the will of the affected person, and if these third persons *de facto* have access to the data. Under Article 32(b), AOL Deutschland (Germany), which stores all e-mails in the United States for cost reasons[54] could, for example, consent to retrieve e-mails from the United States and (if the conditions for the relevant legal basis are fulfilled) to hand them over to the German prosecuting authorities without the need for a letters rogatory from Germany to the United States or the explicit consent of the responsible United States authorities. However, Article 32 (b) does not provide a basis for the coercion of an authorized person like AOL Germany to retrieve the e-mail from abroad. The Convention explicitly requires consent, which by definition contains an element of voluntariness. This applies even if the pre-conditions of the bases of national intervention are fulfilled, which, as a rule, stringently

[52] Article 32 (b) of the Convention reads

> A Party may, without the authorization of another Party, (b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

[53] *See* COUNCIL OF EUROPE, *supra* note 46, n.294 (explaining that "[w]ho is a person that is 'lawfully authorized' to disclose data may vary depending on the circumstances, the nature of the person and the applicable law concerned. For example, a person's e-mail may be stored in another country by a service provider, or a person may intentionally store data in another country. These persons may retrieve the data and, provided that they have the lawful authority, they may voluntarily disclose the data to law enforcement officials or permit such officials to access the data, as provided in the Article.").

[54] Sussmann, *supra* note 17, n.70.

provide for a release of data, as national norms in and of themselves cannot justify a violation of international law.

The question remains of what influence and to what application range the Convention on Cybercrime has on the situation of international law under different possible constellations of consent. Article 32 (b) at least binds the signatory states with respect to international law. It is possible that Article 32 (b), as the result of widely recognized national practices, is thus binding even to non-signatory states as an exercise of international law. The validity of this conclusion depends upon a broadly scattered and representative participation in drafting the treaty, including states whose interests are particularly affected.[55] Much speaks in favor of finding these markers of an international exercise in the Convention: the high number of signatory states, the importance of the signatory states (in which a large part of the infrastructure of the Internet, including storage capacity, is located),[56] as well as the fact that thus far, no caveats regarding Article 32 (b) have been expressed by non-signatory states.[57] Considering the mentioned factors, it can thus be assumed that Article 32 (b) is the result of (newly emerged) international customary law. At the same time, Article 32 (b) does away with the dispute over whether the consent of the affected person is by itself sufficient for undertaking a transborder search or whether, in addition, the consent of the responsible authority of the third country is needed. In the application range of the Convention, Article 32 (b) answers the question in favor of the former. Consequently, a sufficient basis for a transborder search is provided by either the consent of the affected person or of an authorized person in the sense of Article 32 (b).[58]

However, Article 32 does not address the group of transborder searches that is most important in practical considerations: the retrieval of not freely accessible data by a prosecuting authority *without the consent* (or even knowledge) of an authorized person or of the affected country. At the same time, as early as 1995, the Council of Europe proposed the creation of an unambiguous international covenant to avoid international conflicts concerning this matter, and because most states (at least they did at that time) tended to regard this as a violation of sovereignty.[59] According to one member, the G-8 High Tech Crime Subgroup had only shortly thereafter agreed on situations (that were not further specified) in which a transborder search should be permissible without a letters rogatory from the affected country.[60] The governments of the EU member states had also established a common position regarding transborder searches in the Council of Europe, anticipating the negotiations regarding the Convention on Cybercrime. Their position provided that a transborder search for the prosecution of the most severe offenses (to be determined in each individual case) should be permissible in exceptional cases, especially in the case of emergencies.[61] As examples of

[55] *See* International Court of Justice, ICJ Reports 1969, 3, (41 *et seq*., n.70 *et seq*.); MATTHIAS HERDEGEN, VÖLKERRECHT [INTERNATIONAL LAW] § 16 n.9 (2d ed. 2002).

[56] It is a recognized circumstance that in addition to the number, the importance of the states is also significant for the evaluation of whether an exercise of international law exists. *See generally* DOEHRING, *supra* note 38, § 4 n.291 (providing further bibliographic references); HERDEGEN, *supra* note 57, § 16 n.3 (for the parallel case of aerospace law).

[57] The assumption of a corresponding tacit toleration therefore suggests itself; regarding the possibility of the development of an international exercise by way of tacit toleration, see DOEHRING, *supra* note 38, § 4 n.292.

[58] Without Article 32 (b) of the Convention on Cybercrime, however, the consent of the affected person alone would not suffice according to international principles, because an infringement of national sovereignty can only be endorsed by the responsible authorized state authority. A search and seizure of an accused person's apartment at his/her domicile abroad is, for example, not made internationally permissible by the consent of the apartment's owner. In this respect, one would here have to concede to the currently dominant view, if Article 32 (b) of the Convention on Cybercrime did not exist.

[59] *See* Council of Europe, *supra* note 35, Appendix § VII (17); Council of Europe, *supra* note 47, n.189.

[60] *See* Sussmann, *supra* note 17, n.147 (citing Scott Charney).

[61] COUNCIL OF EUROPE, *supra* note 51, at 1. Article 1(7) reads

such emergencies, they suggested the impending deletion or alteration of evidence, or the prevention of an offense which could lead to a person's death or cause severe injuries to a person.[62] Initially, this position was largely supported by the "Committee of Experts on Crime in Cyberspace," a think tank which had been established in the process of devising the Convention on Cybercrime.[63] In the course of the negotiations regarding the Convention it became evident, however, that the participating states would not be able to commit to a binding provision. Finally, the states refrained from establishing a provision going beyond Article 32, because, on the one hand, there was a lack of appropriate previous experience and, on the other hand, a solution satisfying all interests often depends on the specific circumstances of each individual case, which makes the compilation of generally formulated regulations difficult.[64]

Consequently, Article 32 of constitutes the lowest common denominator on which the states involved in the establishment of the Convention could agree. As a result, a reverse conclusion is obtrusive, namely that all transborder searches that are not addressed in Article 32 of the Convention on Cybercrime are impermissible with respect to international law. This conclusion is, however, averted by Article 39, which states that none of the provisions laid down in the Convention shall affect or impair other rights.[65] From the existence of Article 32, one can thus neither conclude the impermissibility nor the permissibility of transborder searches not regulated therein. With the exception of the possible different constellations of consent, Article 32 (b) of the Convention consequently does not offer a response to the question of to what extent a transborder search of or for protected data is permissible under international law.

Because of the lack of additional international treaties or agreements, the only additional recourse is to examine international exercise and practice in order to determine whether and when a transborder search in the case of not freely accessible data is permissible. For this purpose, the Gorshkov-Ivanov case, described earlier, constitutes a classic example. The FBI's course of action in the Gorshkov-Ivanov case allows the conclusion that the United States obviously considers a transborder search a permissible (with respect to international law) prosecutory tool in exceptional cases, such as, ones involving the threat of deletion of evidence of a severe criminal offense. This conclusion is supported by a statement in the USDOJ's manual about electronic evidence, according to which the consent of the responsible foreign authority is principally to be sought,[66] but which also states that extraordinary

> [A] transborder computer search for the purpose of the investigation of a serious criminal offense, to be further defined in the Convention, may be considered in exceptional cases, and in particular where there is an emergency, for example, as far as necessary to prevent the destruction or alteration of evidence of the serious offense, or to prevent the commission of an offense that is likely to result in the death of or serious physical injury to, a person.

[62] *See, e.g.*, Sieber, *Collecting & Using*, *supra* note 7, n.25; Sieber, *Legal Aspects*, *supra* note 7, n.239 (discussing this situation as a further possible and permissible exception from the prohibition of transborder searches).

[63] *See* Dietrich Neumann, *Review on the Instruments of the European Union to Combat Computer Crime and Overview of the Negotiations of the Draft Cyber Crime Convention of the Council of Europe in Strasbourg, at* http://www.oas.org/juridico/english/review_on_the_instruments_of_the.htm (last visited Feb. 20, 2004).

[64] Council of Europe, *supra* note 47, n.293 (stating "The drafters ultimately determined that it was not yet possible to prepare a comprehensive, legally binding regime regulating this area. In part, this was due to a lack of concrete experience with such situations to date; and, in part, this was due to an understanding that the proper solution often turned on the precise circumstances of the individual case, thereby making it difficult to formulate general rules.").

[65] Article 39(3) of the Convention reads "Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party." *See also* Council of Europe, *supra* note 47, n.293 ("stating that Article 39, paragraph 3 provides that other situations are neither authorized, nor precluded.").

[66] *See* USDOJ, SEARCHING & SEIZING, *supra* note 4, 25.

situations such as terrorist threats could, in certain circumstances, open up the possibility of a non-consensual or pre-consensual transborder search.[67] Russia, on the other hand, apparently holds the opposite view, and appears to reject transborder searches. This position is demonstrated by Russia's reactions to the FBI's actions in the Gorshkov-Ivanov case. Accordingly, it is currently not (yet) possible to speak of a (at least largely) standardized international practice or exercise. It is thus to be noted that a transborder search in the case of not freely accessible data cannot rest upon international exercise and practice. A transborder search in this respect is (apart from the possible different constellations of consent) fundamentally impermissible, for want of adequate recognition by one of the legal sources of international law.

This means that the Russian territorial sovereignty was violated by the United States in the Gorshkov-Ivanov case. Therefore, a statement about the influence of the illicitly obtained (with respect to international law) evidence would have been appropriate, at least during the conviction of the two offenders by United States district courts (exclusionary rule regarding the obtained data, ground for mitigation, etc).

An exception from the exclusionary rule applies, however, if the data are stored in the United States and if particular circumstances prevail. The United States assumes that a transborder search is allowed by international law in exceptional cases (whose exceptional character is defined by the United States). While this is unfounded, it shows that the United States would agree to a transborder search procedure in its territory in exceptional circumstances. From the actions taken in the Gorshkov-Ivanov case and from the corresponding statements in the USDOJ's manual of electronic evidence, one can conclude that the United States generally consents to transborder searches even with respect to not freely accessible data, if extraordinary circumstances prevail.[68] If another country then makes use of this option, this state would show through its action that it, too, would tolerate such a course of action in an exceptional case. The Gorshkov-Ivanov case could, in this respect, mark the beginning of the establishment of an international practice or exercise, with which a transborder search with respect to protected data is internationally legally accepted in exceptional cases.

Beyond this, there are no further exceptions from the principle of international impermissibility of transborder searches with respect to not freely accessible data. This also applies for the so-called "good faith" cases, because neither an adequate international treaty nor an international practice or exercise tolerating such a course of action exists – however desirable they may be. Therefore, if it becomes evident later that the principle of territoriality has been violated by the actions of prosecuting authorities, these actions remain contrary to international law. In that case, there exists a possibility of restituting the violation retrospectively, namely by way of an inquiry to the affected state about whether the data may be used. It is, however, impermissible to first access the data for the purpose of a preliminary backup and to only afterwards ask the affected state for permission to utilize the data obtained in violation of international law. This would be a knowing and deliberate violation of effective (international) law, from which prosecuting authorities are enjoined under any circumstances, as they are responsible to the law.

[67] *See id.* at 27 (absolutely in line with Sussmann's airplane example, *supra* note 17 at 453-54).

[68] *See* Koerner, *supra* note 4, at 38 (quoting S. Granick as saying "Basically, the ruling says that our police officers can obtain unauthorized access to a computer for law-enforcement purposes, despite the fact that it is overseas or under the jurisdiction of another country . . . . That could come back to haunt us, when foreign police log onto our citizens' computers in America to take evidence to try them under their laws. Russian intelligence agents, for example, might now feel at liberty to hack American machines in the guise of 'investigations'.").

## III. FINAL REMARKS AND CONCLUSION

The improvements in international cooperation introduced by the Convention on Cybercrime will considerably increase the chances of convicting an offender if he or she leaves behind relevant evidence abroad while committing offenses using the Internet. Despite these improvements, the current situation with respect to unilateral measures is unsatisfactory for cases in which particular exceptional situations make it necessary to rapidly access data stored abroad that is not freely accessible. In these cases, it would be desirable to quickly reach an international, ideally laid out in a protocol supplementary to the Convention on Cybercrime (similar to the supplementary anti-racism protocol). However, it will probably not be possible to implement a contractual agreement of this kind in the near future. In the meantime, an international legal practice corresponding to the principles of the Gorshkov-Ivanov case could arise, which would be a welcome development. But for now, transborder searches with respect to protected data are, in principle, impermissible.