Using a Local Search Warrant to Acquire Evidence Stored Overseas via the Internet

Kenny Wang

Chapter 3

USING A LOCAL SEARCH WARRANT TO ACQUIRE EVIDENCE STORED OVERSEAS VIA THE INTERNET

Kenny Wang

Abstract This paper argues that a search warrant issued by a local court does not have the power to search and seize digital evidence stored overseas but accessible via the Internet. Based on the fact that digital evidence can be altered or erased in a very short time, two scenarios are presented to illustrate the lack of power of a local search warrant to acquire digital evidence overseas. Two solutions are presented to overcome the shortcomings of a local search warrant. These solutions can assist law enforcement agencies around the world in searching and seizing digital evidence stored overseas with speed and accuracy, and in addressing court challenges regarding the admissibility and potential illegality of this evidence.

Keywords: Search warrant, remote cross-border search, webmail

1. Introduction

Computer-related crimes are not a new type of crime in Hong Kong. Hong Kong has had computer crime laws since 1993 [10], but the popularity of information and communications technology in recent years has contributed to an increase in the number of computer-related crimes.

For most individuals, a very important function of computers is to store data. Data used by a computer can be stored in various media such as flash drives, hard disks, compact disks and magnetic tapes. Data can also be stored remotely on a server, which may be situated on the same floor as one's office, or on another floor, another building or even another country. Dealing with data that is stored in another country and accessible only via the Internet (web storage) is more complicated in terms of technology and legal jurisdiction, but it is a growing trend. According to

Hirst [13], "[t]he Internet has an international geographically-borderless nature ... you can find things in it without knowing where they are. The Internet is ambient – nowhere in particular and everywhere at once."

Many law enforcement agencies around the world, including in Hong Kong, have stood up special units to deal with computer-related crimes. Although law enforcement agencies aggressively investigate computer crimes, criminals often avoid detection by utilizing computer technologies. To win these battles, law enforcement needs traditional as well as advanced procedures and tools.

The search warrant is a powerful traditional tool. It empowers law enforcement agents to gain entry into a suspect's premises and to search and seize any items in the premises that may constitute evidence of a crime, including computers. It is increasingly common for criminals to store their information overseas and to access it over the Internet. Is it possible for a law enforcement agent to use a local search warrant to search and seize digital information stored overseas but accessible via the Internet?

This paper analyzes the possibility of using a local search warrant, i.e., a search warrant issued in Hong Kong, to search and seize evidence stored on an overseas computer but accessible via the Internet. More specifically, it focuses on the notion of a "remote cross-border search," which is defined as using a computer within the territory of a country to access and examine data physically stored outside of its boundary [1]. The paper also examines the connection between remote cross-border search and extraterritorial jurisdiction. The goal is to help prevent digital evidence from being excluded by a judge because it was obtained illegally. This not only wastes resources but may also expose law enforcement agents to civil or criminal proceedings.

The paper presents two scenarios and analyzes them in the context of various statutes, case law and legal research to determine whether or not a local search warrant can successfully acquire digital evidence that is stored overseas without raising challenges from defense counsel.

2. Crime Scene

Suppose that a law enforcement agent in Hong Kong is in possession of a search warrant issued by a magistrate. The search warrant empowers him and his colleagues to gain entry into a premises and to search and seize items relevant to the investigation. The target is suspected to have committed fraud. The suspect is a computer expert so it is very likely that his computer contains considerable information related to the case.

The D-Day arrives. The law enforcement agent knocks on the door of the suspect's home. The suspect answers the door. The agent arrests the suspect, cautions the suspect, presents the search warrant, explains it to him and starts the search. The agent sees a notebook computer in the living room. Upon examining the computer, he discovers records of bank accounts and transactions that may be related to the investigation. The agent has found some valuable evidence, but there is more. What is this other evidence?

We consider two scenarios. In the first scenario, the law enforcement agent sees a webmail login page on the computer screen. The suspect has already entered his username and password. All that remains to be done is to hit "Enter" on the keyboard.

In the second scenario, the agent finds a piece of paper on the suspect's desk. The paper contains the name of a webmail service provider (WSP), a username and a password. The agent believes that the username and password belong to the suspect's webmail account, but the suspect remains silent when questioned.

We assume that the WSP is in the United States and some e-mail messages in the webmail account may be vital to the successful prosecution of the suspect. How does the law enforcement agent legally obtain the e-mail evidence so that it is admissible in a Hong Kong court?

3. Scenario 1

This scenario involves jurisdictional issues between Hong Kong and the United States. The suspect has a webmail account with a U.S.-based WSP. The WSP maintains numerous mail servers that store millions, possibly billions, of e-mail messages belonging to users from around the world. All the mail servers are physically located in the United States; thus, the servers and their contents are under U.S. legal jurisdiction. The Hong Kong law enforcement agent wants all relevant information pertaining to the webmail account such as registration details and e-mail contents, but the information is in the United States. How can the law enforcement agent legally acquire the information from overseas?

3.1 Traditional Method

The traditional method for handling the case is to rely on mutual legal assistance (MLA). Two governments sign an MLA whereby each guarantees to provide support to the other on criminal matters. Hong Kong and the United States have an MLA agreement [11]. The agreement includes "executing requests for search and seizure." This makes it possible for the U.S. authority that handles the MLA (U.S. Depart-

ment of Justice (USDoJ)) to search the WSP in the United States and seize the relevant information (including the e-mails) on behalf of the Hong Kong Department of Justice (HKDoJ). Under MLA, the USDoJ obtains the registration details and e-mail messages belonging to the suspect and sends the information to the HKDoJ, who then passes it to the requesting law enforcement agency.

The MLA arrangement is feasible but slow – standard MLA procedures may take weeks, if not months, to complete. During this time, it is very likely that the digital evidence and possibly the suspect himself have vanished. The suspect, who normally can only be detained up to 48 hours after his arrest, would have been released long ago and could use any Internet-ready computer to delete all the evidence in his webmail account. Even if the suspect was charged and remanded in prison, he could arrange for someone else to access his account and delete his e-mails. The suspect would be confident that, by the time the MLA procedures are completed, his deleted e-mails would have been gone for weeks or even months and would not be recoverable. The point is that no matter how efficient MLA procedures are, law enforcement agents can never be sure that they will be able to seize digital evidence stored outside their jurisdiction [1].

Is there any way that the e-mail contents stored overseas can be acquired accurately and with speed so that the evidence is not lost?

3.2 Direct Method

The direct method is to access the suspect's webmail account in the United States simply by clicking the "Enter" key on the keyboard. Having accessed the webmail account, all of the suspect's e-mail messages can be downloaded to his computer in Hong Kong so that they come under Hong Kong jurisdiction. Does the local search warrant empower the law enforcement agent in Hong Kong to access digital evidence stored overseas via the Internet?

The answer is in the negative. Before the "Enter" key is depressed and the e-mail messages are downloaded, the messages are still in the United States. The messages would not have been delivered to the suspect's computer in Hong Kong had the download request not been made. As a result, the digital evidence obtained by the law enforcement agent can be regarded as illegally obtained and subject to challenge in court. Could hitting "Enter" on the keyboard and clicking the mouse a few times have such an impact?

The answer is in the affirmative. It is similar to a situation where law enforcement agents execute a search warrant on a subsidiary office

in a different location from the main office. During their search, the agents discover that the subsidiary has a computer network that links to the main office. If a piece of digital evidence stored on the server of the main office is accessible via the computer network at the subsidiary, what should the agents do? Of course, they should apply for another search warrant to search the main office. The first search warrant does not empower them to obtain digital evidence stored in the main office. As a result, it is unlikely that a local search warrant in Hong Kong would permit an agent to search and seize e-mail messages stored overseas.

Johnson and Post [14] argue that the emergence of the Internet has destroyed not only the power of a government to regulate online behavior but also the legitimacy of a sovereign to "regulate global phenomena." The USDoJ [18] admits that although digital evidence seized remotely from one district to another district may be admitted by U.S. courts, it is a different matter altogether when the evidence is located outside the United States; moreover, remotely searching data stored outside the country is a complicated matter. Clearly, the USDoJ has some reservations regarding the validity of remote cross-border searches.

Graham [12] comments that for certain cyber crimes, such as child pornography and hate speech, an international enforcement jurisdiction is justified. Dauterman [7] argues that a state can assert "reasonable jurisdiction" over a person who commits an offense outside the state as long as it causes harmful effects in the state and if there is a substantial connection between the person and the state, the latter should be reasonable to claim extraterritorial jurisdiction. The Arkansas v. Kirwan case [16] demonstrates that U.S. courts could claim jurisdiction as long as a suspect's conduct or the result of his conduct occurred within the state. Nevertheless, it is doubtful that the e-mail content in our scenario fulfills any of the requirements for extraterritorial jurisdiction. This is because the offense involved is not a universal crime. Also, even if the suspect has a substantial connection with Hong Kong, it would be hard to prove that storing e-mail overseas causes harmful effects in Hong Kong. Hiding criminal evidence may have a harmful effect on the case, but not to the Hong Kong public.

Some U.S. legal scholars favor remote cross-border searches. There is a view that countries like the U.S. long for the unilateral power of remote cross-border searches without assistance from or even the acknowledgement of the country where the data is stored [1]. The United States v. Gorshkov [3] and United States v. Ivanov [19] cases show that, when the need arises, U.S. courts are willing to try overseas cyber criminals even though they were not in a U.S. jurisdiction when they committed their crimes, and the courts may admit the digital evidence even if

it is obtained by a unilateral remote cross-border search [4]. Although these two cases were successfully prosecuted, there is a comment that the Gorshkov case cannot give the "conceptual basis" for the legal issue of cross-border search and seizure because it implies that any country that suffers a crime originating from another country can invade the country's sovereignty by remotely searching and seizing property physically located in that country [4]. Also, there is the possibility that the country that suffered the remote cross-border search could retaliate. In fact, Russia's Federal Security Service brought criminal proceedings against the FBI agent in the Gorshkov case who was responsible for accessing the computers in Russia [5].

Based on the cases cited, it appears that the U.S. judiciary has never denied the possibility of extraterritorial jurisdiction; thus, the validity of remote cross-border search may not face many legal challenges in the United States. Goldsmith [9] even argues that cross-border search is a necessary tool against cyber crime, that there are precedents, and that it is inevitable in order to accommodate new technology. On the other hand, Brenner and Schwerha [4] maintain that it is not clear if U.S. law enforcement agents can "lawfully" use computers in the United States to seize digital evidence stored overseas. They also state that the only certainty is that an agent who has conducted such a seizure can claim that, because the digital evidence could be destroyed or moved, he had to obtain the evidence quickly, possibly even without a search warrant [4]. Of course, it is up to the court to accept this claim.

The 2001 Cybercrime Act of Australia grants power to law enforcement agents to "operate electronic equipment at the warrant premises to access data (including data not held at the premises)" if the data might be relevant to the case and the equipment can be operated without damaging it. This act appears to "legalize" remote cross-border searches in other countries, but it does not say whether the Australian authority allows other countries to do the same to computers on Australian soil.

It is important to note that legislation and arguments that favor remote cross-border searches can lead to a situation where a law enforcement agency in any country that has Internet connectivity would have jurisdiction to lawfully access any data stored on the Internet. Such a situation would likely result in chaos because every country could claim legal jurisdiction to Internet servers around the world. This would severely restrict the freedom of speech because no matter where a person voices his views on the Internet he may have committed an offense (usually political) in some part of the world. The irony is that many in the United States claim that the Internet is an ideal place for freedom of speech, but now it appears that any government in the world can control

any content on the Internet. In fact, if this were to be the case, the U.S. would suffer because any law enforcement agency in the world – from Canada, France, China, Peru, even Iran – could claim jurisdiction over all U.S.-based servers with Internet connections.

In the international arena, law enforcement agents from one country cannot exercise their power in the territory of a second country except with the consent of the government of the second country [1]. Berman [2] comments that a target state of a remote cross-border search may feel that the extraterritorial investigations by other states threaten its citizens and may, therefore, impose measures such as privacy protection to limit the scope of investigations or even bar the investigations. In general, a unilateral remote cross-border search violates customary international law [1].

Recognizing the problems associated with MLA, the Council of Europe has suggested various measures for the smooth transfer of digital evidence between states. In 2001, the Council of Europe's Convention on Cybercrime [6] recommended that a speedy MLA such as fax or e-mail should be used to facilitate the rapid preservation of digital evidence. Article 32 of the Convention on Cybercrime legalizes remote cross-border searches of publicly-available data and other data with the consent of the local authority. Nevertheless, the data in our scenario is not publicly available and seeking WSP content may be fruitless. The WSP does not have any legal obligation to comply with a request from overseas and the WSP is not the owner of the data, so it may not even have the authority to give consent to an overseas authority. Thus, it appears that Article 32 does not provide much assistance in our scenario.

Based on our analysis, the problems related to traditional MLA remain. The Hong Kong law enforcement agent may not unilaterally conduct a remote cross-border search on the suspect's webmail account to avoid the embarrassment that the evidence obtained is inadmissible because an offense was committed by the law enforcement agent during its extraction [21].

Is there a better approach? We analyze the second scenario before presenting two solutions.

4. Scenario 2

This scenario differs from the first scenario in that the law enforcement agent has the username and password of the suspect's webmail account. But the problem is that the search warrant is not valid unless it has an extraterritorial effect. Moreover, it is not feasible for the agent to apply for another search warrant because there is nothing local to search.

Conducting a remote cross-border search and seizure using the suspect's username and password is similar to using a key found in the suspect's premises to open the suspect's safe deposit box in a bank. The matter is more complicated if the safe deposit box is located overseas. It is inconceivable that the law enforcement agent would travel to the country where the deposit box is located, open the deposit box and bring its contents back to Hong Kong. The agent does not have the power to search and seize items in another country. Although it can be argued in this scenario that the law enforcement agent has not left his jurisdiction and is, therefore, not acting without authority, it is doubtful that the evidence acquired via the Internet would be admissible in court.

5. Two Solutions

Based on the preceding analysis, we should recognize that, although it is technically feasible to conduct a remote cross-border search and seizure, it is an exception rather than a rule for the court to accept the digital evidence. We present two solutions. Note that these solutions are not related to the illegality of the contents (e.g., pornography or hate speech) as in our hypothetical scenarios. Indeed, there is nothing wrong with the e-mail content *per se*. It is just that the suspect has stored his criminal evidence abroad hoping to take advantage of the jurisdictional restrictions imposed on Hong Kong law enforcement.

5.1 Solution 1

The first solution involves duress, but it has been implemented. The Bank of Nova Scotia case [17] demonstrates that, if necessary, U.S. courts are willing to compel foreign banks with U.S. branches to produce bank records held outside the United States that are subject to foreign jurisdiction. Similarly, a magistrate or judge in Hong Kong could issue a local search warrant to search the Hong Kong subsidiary of the WSP (if one exists), and compel it to produce information about the suspect's webmail account and the contents of all e-mail messages. The rationale is that the webmail account, no matter where it is physically located, is treated as a local webmail account. As long as the owner of the webmail account can access it in Hong Kong, courts would ignore where the webmail account and its contents reside and compel the local subsidiary of the WSP to disclose everything about the account.

Because the evidence is given by the Hong Kong subsidiary, it is treated as evidence obtained locally, so the jurisdictional issue does not arise. While this solution appears to eliminate the jurisdictional problem, the irony is that it turns a blind eye to the issue of extraterritorial

jurisdiction. As a result, multinational companies such as Yahoo or Microsoft would suffer.

Another important point regarding this solution is that the country that uses it must have strong economic bargaining power that would force multinationals to comply; otherwise the companies could pull out and move to a "friendlier" country. Nevertheless, this solution sets aside the problem of extraterritorial jurisdiction and enables a local search warrant to acquire digital evidence stored outside the jurisdiction.

5.2 Solution 2

The second solution attempts to strike a balance between speed and jurisdictional issues; also, it emphasizes the integrity of evidence. In this solution, the Hong Kong law enforcement agent may search and seize the digital evidence immediately using the suspect's computer or using the information on the piece of paper that contains the suspect's webmail username and password. Having seized the evidence, the law enforcement agent should contact the WSP in the United States by fax or e-mail to request the immediate preservation of evidence in the suspect's webmail account pending MLA approval. Meanwhile, the agent should issue a formal MLA request [20]. This solution is different from the one described in Article 32 of the Convention on Cybercrime because it does not require "lawful and voluntary consent" by the WSP. Note that the WSP will only preserve the digital evidence; it will not surrender the evidence to the Hong Kong agent until and unless ordered to do so by a U.S. court under the MLA request.

This solution preserves digital evidence before it can be deleted. Of course, if the evidence from the WSP is the same as that seized in Hong Kong, the evidence from the WSP can be presented to the court directly. However, in the unlikely event that the evidence from the WSP is different from the evidence seized in Hong Kong, more weight should be given to the evidence from the WSP.

This solution is attractive because it conforms with MLA practices. Also, the evidence is preserved speedily and its integrity cannot be questioned because the preservation is done by the WSP, not by the Hong Kong law enforcement agent.

6. Conclusions

The two solutions presented to overcome the shortcomings of a local search warrant are far from perfect. As long as there are cross-border searches on the Internet, there will be debates on how to maintain law and order in cyberspace without infringing the jurisdiction of another

country and the privacy of its citizens. While it is useful to consider streamlining current legal procedures for acquiring digital evidence overseas, in the long term it is important to deal with this issue in the context of MLA agreements. This means that countries may have to negotiate and agree on joint cross-border searches over the Internet. Joint operations require good intelligence and coordination or they could lead to disastrous consequence as in Operation Ore, where thousands of British men were suspected of accessing child porn websites based on credit card payments, when, in fact, some of them were victims of credit card fraud [15]. The European Union provides a good example of transnational cooperation. The European Union has established a border-free travel zone based on its confidence in the border control procedures of its member states [8]; similar confidence could be placed on its member law enforcement agencies in conducting remote cross-border searches over the Internet.

The emergence of cloud computing poses significant problems for law enforcement agencies. If the WSP engages a cloud computing service provider, its customer data could be stored in data servers around the world. As a result, the law enforcement agent cannot recover any digital evidence from the suspect's computer and from the WSP's servers. Even worse, the WSP would not know the exact physical location of the suspect's data.

Interestingly, our two solutions may work even better in a cloud computing environment. In the first solution, since the exact physical location of the suspect's data is almost impossible to determine, the law enforcement agent has a stronger justification to request the local subsidiary of the WSP to produce the suspect's data regardless of where it is actually stored. In the second solution, the WSP has an urgent need to preserve the suspect's data pending MLA. Because the storage of the suspect's data is outside its control, the WSP has to take steps to preserve the suspect's data immediately or there would be no guarantee that it could produce the suspect's data when the court order arrives.

Countries must address the issue of remote cross-border searches before they encounter increasing numbers of unilateral remote cross-border searches from other countries. If countries with advanced technology do not take the initiative immediately, they may be forced to accept solutions imposed by other countries.

References

[1] P. Bellia, Chasing bits across borders, *University of Chicago Legal Forum*, vol. 2001, pp. 35–101, 2001.

[2] P. Berman, The globalization of jurisdiction, *University of Pennsylvania Law Review*, vol. 151, pp. 311–529, 2002.

[3] S. Brenner and B. Koops, Approaches to cybercrime jurisdiction, *Journal of High Technology Law*, vol. 4(1), 2004.

[4] S. Brenner and J. Schwerha, Transnational evidence gathering and local prosecution of international cybercrime, *John Marshall Journal of Computer and International Law*, vol. 20(3), pp. 347–395, 2002.

[5] M. Brunker, FBI agent charged with hacking, msnbc.com, New York (www.msnbc.msn.com/id/3078784), August 15, 2002.

[6] Council of Europe, Convention on Cybercrime, ETS No. 185, Strasbourg, France (conventions.coe.int/Treaty/EN/Treaties/Html/185.htm), 2001.

[7] W. Dauterman, Internet regulation: Foreign actors and local harms – At the crossroads of pornography, hate speech and freedom of expression, *North Carolina Journal of International Law and Commercial Regulation*, vol. 28(1), pp. 177–203, 2002.

[8] Financial Times, Schengen at 24, London, United Kingdom (www.ft.com/cms/s/bce06dec-af2f-11dc-880f-0000779fd2ac.html), December 20, 2007.

[9] J. Goldsmith, The Internet and the legitimacy of remote cross-border searches, *University of Chicago Legal Forum*, vol. 2001, pp. 103–118, 2001.

[10] Government of the Hong Kong Special Administrative Region, Computer Crimes Ordinance, Hong Kong (www.infosec.gov.hk/english/ordinances/corresponding.html), 1993.

[11] Government of the Hong Kong Special Administrative Region, Mutual Legal Assistance in Criminal Matters (United States of America) Order, Chapter 525F, Hong Kong (www.legislation.gov.hk/blis_pdf.nsf/6799165D2FEE3FA94825755E0033E532/E002F63F30772ED5482575EF0013F89F?OpenDocument&bt=0), 2000.

[12] W. Graham, Uncovering and eliminating child pornography rings on the Internet: Issues regarding and avenues facilitating law enforcement's access to "Wonderland," *Detroit College of Law at Michigan State University Law Review*, vol. 2, pp. 457–484, 2000.

[13] M. Hirst, *Jurisdiction and the Ambit of the Criminal Law*, Oxford University Press, Oxford, United Kingdom, 2003.

[14] D. Johnson and D. Post, Law and borders: The rise of law in cyberspace, *Stanford Law Review*, vol. 48(5), pp. 1367–1402, 1996.

[15] S. Laville, Legal challenge to web child abuse inquiry, guardian .co.uk, London, United Kingdom (www.guardian.co.uk/uk/2009 /jul/02/web-child-abuse-inquiry-challenge), July 2, 2009.

[16] Supreme Court of Arkansas, Kirwan v. State of Arkansas, *South Western Reporter (Third Series)*, vol. 96, pp. 724–731, 2003.

[17] U.S. Court of Appeals (Eleventh Circuit), United States v. Bank of Nova Scotia, *Federal Reporter (Second Series)*, vol. 740, pp. 817–832, 1984.

[18] U.S. Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Office of Legal Education, Executive Office for United States Attorneys, Washington, DC (www.justice.gov/criminal/cybercrime/ssmanual /ssmanual2009.pdf), 2009.

[19] U.S. District Court (District of Connecticut), United States v. Ivanov, *Federal Supplement (Second Series)*, vol. 175, pp. 367–375, 2001.

[20] U.S. Government, Title 18, Section 2703, *United States Code Annotated, Cumulative Annual Pocket Part*, pp. 87–93, 2009.

[21] E. Wilding, *Computer Evidence: A Forensic Investigation Handbook*, Sweet and Maxwell, London, United Kingdom, 1997.