EXHIBIT L

Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations

H. Marshall Jarrett
Director, EOUSA

Michael W. Bailie
Director, OLE

OLE Litigation Series

Ed Hagen
Assistant Director, OLE

Nathan Judish
Computer Crime and Intellectual Property Section

Computer Crime and
Intellectual Property Section
Criminal Division

Published by
Office of Legal Education
Executive Office for
United States Attorneys

The Office of Legal Education intends that this book be used by Federal prosecutors for training and law enforcement purposes.

The contents of this book provide internal suggestions to Department of Justice attorneys. Nothing in it is intended to create any substantive or procedural rights, privileges, or benefits enforceable in any administrative, civil, or criminal matter by any prospective or actual witnesses or parties. *See United States v. Caceres*, 440 U.S. 741 (1979).

Table of Contents

Preface and Acknowledgements vii

Introduction ix

Chapter 1. Searching and Seizing Computers Without a Warrant 1

A. Introduction 1
B. The Fourth Amendment's "Reasonable Expectation of Privacy" in Cases Involving Computers 2
1. General Principles 2
2. Reasonable Expectation of Privacy in Computers as Storage Devices 2
3. Reasonable Expectation of Privacy and Third-Party Possession 6
4. Private Searches 10
5. Use of Specialized Technology to Obtain Information 14
C. Exceptions to the Warrant Requirement in Cases Involving Computers 15
1. Consent 15
2. Exigent Circumstances 27
3. Search Incident to a Lawful Arrest 31
4. Plain View 34
5. Inventory Searches 37
6. Border Searches 38
7. Probation and Parole 40
D. Special Case: Workplace Searches 42
1. Private-Sector Workplace Searches 42
2. Public-Sector Workplace Searches 45
E. International Issues 56

Chapter 2. Searching and Seizing Computers With a Warrant 61

A. Introduction 61
B. Devising a Search Strategy 61
C. Drafting the Affidavit, Application, and Warrant 63
1. Include Facts Establishing Probable Cause 63
2. Describe With Particularity the Things to be Seized 69

3. Establishing the Necessity for Imaging and Off-Site Examination 76
4. Do Not Place Limitations on the Forensic Techniques That May Be Used To Search 79
5. Seeking Authorization for Delayed Notification Search Warrants ... 83
6. Multiple Warrants in Network Searches 84
D. Forensic Analysis 86
1. The Two-Stage Search 86
2. Searching Among Commingled Records 87
3. Analysis Using Forensic Software 89
4. Changes of Focus and the Need for New Warrants 90
5. Permissible Time Period for Examining Seized Media 91
6. Contents of Rule 41(f) Inventory Filed With the Court 95
E. Challenges to the Search Process 96
1. Challenges Based on "Flagrant Disregard" 96
2. Motions for Return of Property 98
F. Legal Limitations on the Use of Search Warrants to Search Computers 100
1. Journalists and Authors: the Privacy Protection Act 101
2. Privileged Documents 109
3. Other Disinterested Third Parties 111
4. Communications Service Providers: the SCA 112

Chapter 3. The Stored Communications Act 115
A. Introduction 115
B. Providers of Electronic Communication Service vs. Remote Computing Service 117
1. Electronic Communication Service 117
2. Remote Computing Service 119
C. Classifying Types of Information Held by Service Providers 120
1. Basic Subscriber and Session Information Listed in 18 U.S.C. § 2703(c)(2) 121
2. Records or Other Information Pertaining to a Customer or Subscriber 122
3. Contents and "Electronic Storage" 122
4. Illustration of the SCA's Classifications in the Email Context 125
D. Compelled Disclosure Under the SCA 127
1. Subpoena 128

2. Subpoena with Prior Notice to the Subscriber or Customer 129
3. Section 2703(d) Order 130
4. 2703(d) Order with Prior Notice to the Subscriber or Customer ... 132
5. Search Warrant 133
E. Voluntary Disclosure 135
F. Quick Reference Guide 138
G. Working with Network Providers: Preservation of Evidence, Preventing Disclosure to Subjects, Cable Act Issues, and Reimbursement 139
1. Preservation of Evidence under 18 U.S.C. § 2703(f) 139
2. Orders Not to Disclose the Existence of a Warrant, Subpoena, or Court Order 140
3. The Cable Act, 47 U.S.C. § 551 141
4. Reimbursement 142
H. Constitutional Considerations 144
I. Remedies 147
1. Suppression 147
2. Civil Actions and Disclosures 148

Chapter 4. Electronic Surveillance in Communications Networks 151
A. Introduction 151
B. Content vs. Addressing Information 151
C. The Pen/Trap Statute, 18 U.S.C. §§ 3121-3127 153
1. Definition of Pen Register and Trap and Trace Device 153
2. Pen/Trap Orders: Application, Issuance, Service, and Reporting ... 154
3. Emergency Pen/Traps 158
4. The Pen/Trap Statute and Cell-Site Information 159
D. The Wiretap Statute ("Title III"), 18 U.S.C. §§ 2510-2522 161
1. Introduction: The General Prohibition 161
2. Key Phrases 162
3. Exceptions to Title III's Prohibition 167
E. Remedies For Violations of Title III and the Pen/Trap Statute 183
1. Suppression Remedies 183
2. Defenses to Civil and Criminal Actions 188

Chapter 5. Evidence 191
A. Introduction 191
B. Hearsay 191
1. Hearsay vs. Non-Hearsay Computer Records 192
2. Confrontation Clause 196
C. Authentication 197
1. Authentication of Computer-Stored Records 198
2. Authentication of Records Created by a Computer Process 200
3. Common Challenges to Authenticity 202
D. Other Issues 205
1. The Best Evidence Rule 205
2. Computer Printouts as "Summaries" 207

Appendices
A. Sample Network Banner Language 209
B. Sample 18 U.S.C. § 2703(d) Application and Order 213
C. Sample Language for Preservation Requests under 18 U.S.C. § 2703(f) 225
D. Sample Pen Register/Trap and Trace Application and Order 227
E. Sample Subpoena Language 239
F. Sample Premises Computer Search Warrant Affidavit 241
G. Sample Letter for Provider Monitoring 251
H. Sample Authorization for Monitoring of Computer Trespasser Activity 253
I. Sample Email Account Search Warrant Affidavit 255
J. Sample Consent Form for Computer Search 263

Table of Cases 265

Index 281

[Pages v – 212 omitted]

Appendix B
Sample 18 U.S.C. § 2703(d) Application and Order

Note that this sample 2703(d) application and order are for the disclosure of both content and non-content information associated with an email account at an ISP.

When using a 2703(d) order to compel disclosure of content, the government is required either to give prior notice to the subscriber or customer or to comply with the procedures for delayed notice in 18 U.S.C. § 2705(a). This order authorizes the delay of notice to the account holder under 18 U.S.C. § 2705(a). A 2703(d) order can be used to compel disclosure of the content of communications not in "electronic storage" or the content of communications in "electronic storage" for more than 180 days. As discussed in Chapter 3.C.3, courts disagree on whether previously retrieved communications fall within the scope of communications in "electronic storage."

When a 2703(d) order is used to compel disclosure only of non-content information, no notice to the customer or subscriber is required.

UNITED STATES DISTRICT COURT
FOR THE [DISTRICT}

IN RE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d)	MISC. NO. ____
	Filed Under Seal

APPLICATION OF THE UNITED STATES FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d)

The United States of America, moving by and through its undersigned

counsel, respectfully submits under seal this ex parte application for an Order pursuant to 18 U.S.C. § 2703(d) to require ISPCompany, an Internet Service Provider located in City, State, which functions as an electronic communications service provider and/or a remote computing service, to provide records and other information and contents of wire or electronic communications pertaining to the following email account: sample@sample.com. The records and other information requested are set forth as an Attachment to the proposed Order. In support of this application, the United States asserts:

LEGAL AND FACTUAL BACKGROUND

1. The United States government is investigating [crime summary]. The investigation concerns possible violations of, inter alia, [statutes].

2. Investigation to date of these incidents provides reasonable grounds to believe that ISPCompany has records and other information pertaining to certain of its subscribers that are relevant and material to an ongoing criminal investigation. Because ISPCompany functions as an electronic communications service provider (provides its subscribers access to electronic communication services, including email and the Internet) and/or a remote computing service (provides computer facilities for the storage and processing of electronic communications), 18 U.S.C. § 2703 sets out particular requirements that the government must meet in order to obtain access to the records and other information it is seeking.

3. Here, the government seeks to obtain the following categories of information: (1) records and other information (not including the contents of

communications) pertaining to certain subscribers of ISPCompany; and (2) the contents of electronic communications held by ISPCompany (but not in electronic storage for less than 181 days).

4. To obtain records and other information (not including the contents of communications) pertaining to subscribers of an electronic communications service provider or remote computing service, the government must comply with 18 U.S.C. § 2703(c)(1), which provides, in pertinent part:

> A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—
> . . . .
>
> (B) obtains a court order for such disclosure under subsection (d) of this section.

5. Under 18 U.S.C. § 2703(a)(1) and 18 U.S.C. § 2703(b)(1), to obtain the contents of a wire or electronic communication in a remote computing service, or in electronic storage for more than one hundred and eighty days in an electronic communications system, the government must comply with 18 U.S.C. § 2703(b)(1), which provides, in pertinent part:

> A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—
> . . . .
>
> (B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—
> . . . .

> (ii) obtains a court order for such disclosure under subsection (d) of this section;
>
> except that delayed notice may be given pursuant to section 2705 of this title.

6. Section 2703(b)(2) states that § 2703(b)(1) applies with respect to any wire or electronic communication that is held or maintained in a remote computing service—

> (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and
>
> (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

7. Section 2703(d), in turn, provides in pertinent part:

> A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction[1] and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. . . . A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually

[1] 18 U.S.C. § 2711(3) states that "the term 'court of competent jurisdiction' has the meaning assigned by section 3127, and includes any Federal court within that definition, without geographic limitation." Section 3127 defines the term "court of competent jurisdiction" to include "any district court of the United States (including a magistrate judge of such a court)." 18 U.S.C. § 3127(2)(A).

> voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

Accordingly, this application sets forth specific and articulable facts showing that there are reasonable grounds to believe that the materials sought are relevant and material to an ongoing criminal investigation.

THE RELEVANT FACTS

8. [Factual paragraph(s) here]

9. The conduct described above provides reasonable grounds to believe that the materials sought are relevant and material to an ongoing criminal investigation.

10. Records of customer and subscriber information relating to this investigation that are available from ISPCompany, and the contents of electronic communications that may be found at ISPCompany, will help government investigators to identify the individual(s) who are responsible for the events described above and to determine the nature and scope of their activities. Accordingly, the government requests that ISPCompany be directed to produce all records described in Attachment A to the proposed Order. Part A of the Attachment requests the account name, address, telephone number, email address, billing information, and other identifying information for sample@sample.com.

11. Part B requests the production of records and other information relating to sample@sample.com through the date of this Court's Order. As described in more detail in that section, this information should include connection

information, telephone records, non-content information associated with any communication or file stored by or for the account(s), and correspondence and notes of records involving the account.

12. Part C requests the contents of electronic communications (not in electronic storage) in ISPCompany's computer systems in directories or files owned or controlled by the accounts identified in Part A. These stored files, covered by 18 U.S.C. § 2703(b)(2), will help ascertain the scope and nature of the activity conducted by sample@sample.com from ISPCompany's computers. Pursuant to 18 U.S.C. § 2703(a), Part C also requests the contents of electronic communications that have been in electronic storage in ISPCompany's computer systems for more than 180 days.

13. The information requested should be readily accessible to ISPCompany by computer search, and its production should not prove to be burdensome.

14. The United States requests that this application and Order be sealed by the Court until such time as the Court directs otherwise.

15. The United States requests that pursuant to the preclusion of notice provisions of 18 U.S.C. § 2705(b), ISPCompany be ordered not to notify any person (including the subscriber or customer to which the materials relate) of the existence of this Order for such period as the Court deems appropriate. The United States submits that such an order is justified because notification of the existence of this Order would seriously jeopardize the ongoing investigation. Such a disclosure would give the subscriber an opportunity to destroy evidence,

change patterns of behavior, notify confederates, or flee or continue his flight from prosecution.

16. The United States further requests, pursuant to the delayed notice provisions of 18 U.S.C. § 2705(a), an order delaying any notification to the subscriber or customer that may be required by § 2703(b) to obtain the contents of communications, for a period of ninety days. Providing prior notice to the subscriber or customer would seriously jeopardize the ongoing investigation, as such a disclosure would give the subscriber an opportunity to destroy evidence, change patterns of behavior, notify confederates, or flee or continue his flight from prosecution.

WHEREFORE, it is respectfully requested that the Court grant the attached Order (1) directing ISPCompany to provide the United States with the records and information described in Attachment A; (2) directing that the application and Order be sealed; (3) directing ISPCompany not to disclose the existence or content of the Order or this investigation, except to the extent necessary to carry out the Order; and (4) directing that the notification by the government otherwise required under 18 U.S.C. § 2703(b) be delayed for ninety days; and (5) directing that three certified copies of this application and Order be provided by the Clerk of this Court to the United States Attorney's Office.

Executed on _____

_____
Assistant United States Attorney

UNITED STATES DISTRICT COURT
FOR THE _____

IN RE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d)	)	MISC. NO.
	)	Filed Under Seal

ORDER

This matter having come before the Court pursuant to an application under Title 18, United States Code, Section 2703, which application requests the issuance of an order under Title 18, United States Code, Section 2703(d) directing ISPCompany, an electronic communications service provider and/or a remote computing service, located in City, State, to disclose certain records and other information, as set forth in Attachment A to this Order, the Court finds that the applicant has offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information and the contents of wire or electronic communications sought are relevant and material to an ongoing criminal investigation.

IT APPEARING that the information sought is relevant and material to an ongoing criminal investigation, and that prior notice to any person of this investigation or this application and Order entered in connection therewith would seriously jeopardize the investigation;

IT IS ORDERED pursuant to Title 18, United States Code, Section 2703(d) that ISPCompany will, within seven days of the date of this Order,

turn over to the United States the records and other information as set forth in Attachment A to this Order.

IT IS FURTHER ORDERED that the Clerk of the Court shall provide the United States Attorney's Office with three (3) certified copies of this application and Order.

IT IS FURTHER ORDERED that the application and this Order are sealed until otherwise ordered by the Court, and that ISPCompany shall not disclose the existence of the application or this Order of the Court, or the existence of the investigation, to the listed subscriber or to any other person, unless and until authorized to do so by the Court.

IT IS FURTHER ORDERED that the notification by the government otherwise required under 18 U.S.C. § 2703(b)(1)(B) be delayed for a period of ninety days.

_____ _____

United States Magistrate Judge Date

ATTACHMENT A

You are to provide the following information, if available, as data files on CD-ROM or other electronic media or by facsimile:

A. The following customer or subscriber account information for each account registered to or associated with sample@sample.com for the time period [date range]:

1. subscriber names, user names, screen names, or other identities;
2. mailing addresses, residential addresses, business addresses, email addresses, and other contact information;
3. local and long distance telephone connection records, or records of session times and durations;
4. length of service (including start date) and types of service utilized;
5. telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
6. means and source of payment for such service (including any credit card or bank account number) and billing records.

B. All records and other information relating to the account(s) and time period in Part A, including:

1. records of user activity for any connections made to or from the account, including the date, time, length, and method of connections, data transfer volume, user name, and source and destination Internet Protocol address(es);
2. telephone records, including caller identification records, cellular site and sector information, GPS data, and cellular network identifying information (such as the IMSI, MSISDN, IMEI, MEID, or

ESN);

3. non-content information associated with the contents of any communication or file stored by or for the account(s), such as the source and destination email addresses and IP addresses.
4. correspondence and notes of records related to the account(s).

C. [Before seeking to compel disclosure of content, give prior notice to the customer or subscriber *or* comply with the delayed notice provisions of 18 U.S.C. § 2705(a).] The contents of electronic communications (not in electronic storage[2]) in ISPCompany's systems in directories or files owned or controlled by the accounts identified in Part A at any time from [date range]; and the contents of electronic communications that have been in electronic storage in ISPCompany's electronic communications system for more than 180 days [and within date range].

[2] "Electronic storage" is a term of art, specifically defined in 18 U.S.C. § 2510(17) as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." The government does not seek access to any communications in "electronic storage" for less than 181 days. [**The following sentence may not be included in the Ninth Circuit; see the discussion of "electronic storage" in Chapter 3.C.3.**] Communications not in "electronic storage" include any email communications received by the specified accounts that the owner or user of the account has already accessed, viewed, or downloaded.