RIF

Effective: October 13, 2008

United States Code Annotated Currentness
Title 18. Crimes and Criminal Procedure (Refs & Annos)
Part I. Crimes (Refs & Annos)
Chapter 121. Stored Wire and Electronic Communications and Transactional Records Access (Refs & Annos)

§ 2702. Voluntary disclosure of customer communications or records

(a) Prohibitions.--Except as provided in subsection (b) or (c)--

(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and

(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that 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 service;

(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; and

(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.

(b) Exceptions for disclosure of communications.-- A provider described in subsection (a) may divulge the contents of a communication--

(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

(2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;

(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

RIF

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A;

(7) to a law enforcement agency--

(A) if the contents--

(i) were inadvertently obtained by the service provider; and

(ii) appear to pertain to the commission of a crime; or

[**(B)** Repealed. Pub.L. 108-21, Title V, § 508(b)(1)(A), Apr. 30, 2003, 117 Stat. 684]

[**(C)** Repealed. Pub.L. 107-296, Title II, § 225(d)(1)(C), Nov. 25, 2002, 116 Stat. 2157]

(8) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.

(c) Exceptions for disclosure of customer records.--A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))--

(1) as otherwise authorized in section 2703;

(2) with the lawful consent of the customer or subscriber;

(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(4) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency;

(5) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A; or

(6) to any person other than a governmental entity.

(d) Reporting of emergency disclosures.--On an annual basis, the Attorney General shall submit to the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate a report containing--

(1) the number of accounts from which the Department of Justice has received voluntary disclosures under subsection (b)(8); and

RTF

(2) a summary of the basis for disclosure in those instances where--

(A) voluntary disclosures under subsection (b)(8) were made to the Department of Justice; and

(B) the investigation pertaining to those disclosures was closed without the filing of criminal charges.

CREDIT(S)

(Added Pub.L. 99-508, Title II, § 201[a], Oct. 21, 1986, 100 Stat. 1860, and amended Pub.L. 100-690, Title VII, § 7037, Nov. 18, 1988, 102 Stat. 4399; Pub.L. 105-314, Title VI, § 604(b), Oct. 30, 1998, 112 Stat. 2984; Pub.L. 107-56, Title II, § 212(a)(1), Oct. 26, 2001, 115 Stat. 284; Pub.L. 107-296, Title II, § 225(d)(1), Nov. 25, 2002, 116 Stat. 2157; Pub.L. 108-21, Title V, § 508(b), Apr. 30, 2003, Stat. 684; Pub.L. 109-177, Title I, § 107(a), (b)(1), (c), Mar. 9, 2006, 120 Stat. 202, 203; Pub.L. 110-401, Title V, § 501(b)(2), Oct. 13, 2008, 122 Stat. 4251.)

Current through P.L. 112-3 (excluding P.L. 111-296, 111-314, 111-320, 111-350, 111-377, and 111-383) approved 2-25-11

END OF DOCUMENT

RTF

Effective: October 19, 2009

United States Code Annotated Currentness
Title 18. Crimes and Criminal Procedure (Refs & Annos)
Part I. Crimes (Refs & Annos)
Chapter 121. Stored Wire and Electronic Communications and Transactional Records Access (Refs & Annos)

§ 2703. Required disclosure of customer communications or records

(a) Contents of wire or electronic communications in electronic storage.--A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) Contents of wire or electronic communications in a remote computing service.--(1) 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--

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity--

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(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.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that 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

RIF

(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.

(c) Records concerning electronic communication service or remote computing service.--(1) 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--

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction;

(B) obtains a court order for such disclosure under subsection (d) of this section;

(C) has the consent of the subscriber or customer to such disclosure;

(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the--

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

(d) Requirements for court order.--A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction 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. In

the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. 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 voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

(e) No cause of action against a provider disclosing information under this chapter.--No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.

(f) Requirement to preserve evidence.--

(1) In general.--A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) Period of retention.--Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

(g) Presence of officer not required.--Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

CREDIT(S)

(Added Pub.L. 99-508, Title II, § 201[a], Oct. 21, 1986, 100 Stat. 1861, and amended Pub.L. 100-690, Title VII, §§ 7038, 7039, Nov. 18, 1988, 102 Stat. 4399; Pub.L. 103-322, Title XXXIII, § 330003(b), Sept. 13, 1994, 108 Stat. 2140; Pub.L. 103-414, Title II, § 207(a), Oct. 25, 1994, 108 Stat. 4292; Pub.L. 104-132, Title VIII, § 804, Apr. 24, 1996, 110 Stat. 1305; Pub.L. 104-293, Title VI, § 601(b), Oct. 11, 1996, 110 Stat. 3469; Pub.L. 104-294, Title VI, § 605(f), Oct. 11, 1996, 110 Stat. 3510; Pub.L. 105-184, § 8, June 23, 1998, 112 Stat. 522; Pub.L. 107-56, Title II, §§ 209(2), 210, 212(b)(1), 220(a)(1), (b), Oct. 26, 2001, 115 Stat. 283, 285, 291, 292; Pub.L. 107-273, Div. B, Title IV, § 4005(a)(2), Div. C, Title I, § 11010, Nov. 2, 2002, 116 Stat. 1812, 1822; Pub.L. 107-296, Title II, § 225(h)(1), Nov. 25, 2002, 116 Stat. 2158; Pub.L. 109-162, Title XI, § 1171(a)(1), Jan. 5, 2006, 119 Stat. 3123; Pub.L. 111-79, § 2(1), Oct. 19, 2009, 123 Stat. 2086.)

HISTORICAL AND STATUTORY NOTES

Revision Notes and Legislative Reports

1986 Acts. Senate Report No. 99-541, see 1986 U.S. Code Cong. and Adm. News, p. 3555.

1988 Acts. For Related Reports, see 1988 U.S. Code Cong. and Adm. News, p. 5937.

1994 Acts. House Report Nos. 103-324, 103-489, and House Conference Report No. 103-711, see 1994 U.S. Code Cong. and Adm. News, p. 1801.

House Report No. 103-827, see 1994 U.S. Code Cong. and Adm. News, p. 3489.

RIF

1996 Acts. Senate Report No. 104-179 and House Conference Report No. 104-518, see 1996 U.S. Code Cong. and Adm. News, p. 924.

Senate Report Nos. 104-258, 104-277, 104-337 and House Conference Report No. 104-832, see 1996 U.S. Code Cong. and Adm. News, p. 3945.

House Report No. 104-788, see 1996 U.S. Code Cong. and Adm. News, p. 4021.

1998 Acts. House Report No. 105-158, see 1998 U.S. Code Cong. and Adm. News, p. 231.

2002 Acts. House Conference Report No. 107-685 and Statement by President, see 2002 U.S. Code Cong. and Adm. News, p. 1120.

House Report No. 107-609(Part I) and Statement by President, see 2002 U.S. Code Cong. and Adm. News, p. 1352.

2006 Acts. House Report No. 109-233, see 2005 U.S. Code Cong. and Adm. News, p. 1636.

Amendments

2009 Amendments. Subsec. (a). Pub.L. 111-79, § 2(1)(A), struck out "by a court with jurisdiction over the offense under investigation or an equivalent State warrant" and inserted "(or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction".

Subsec. (b)(1)(A). Pub.L. 111-79, § 2(1)(B), struck out "by a court with jurisdiction over the offense under investigation or an equivalent State warrant" and inserted "(or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction".

Subsec. (c)(1)(A). Pub.L. 111-79, § 2(1)(C), struck out "by a court with jurisdiction over the offense under investigation or an equivalent State warrant" and inserted "(or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction".

2006 Amendments. Subsec. (c)(1)(C). Pub.L. 109-162, § 1171(a)(1), struck out "or" at the end.

2002 Amendments. Subsec. (c)(1)(E). Pub.L. 107-273, § 4005(a)(2), adjusted the margins and thus required no change in text.

Subsec. (e). Pub.L. 107-296, § 225(h)(1), inserted ", statutory authorization" following "subpoena".

Subsec. (g). Pub.L. 107-273, § 11010, added subsec. (g).

2001 Amendments. Catchline. Pub.L. 107-56, § 212(b)(1)(A), rewrote the catchline, which formerly read "Requirements for governmental access".

Subsecs. (a), (b). Pub.L. 107-56, § 209(2), struck out "Contents of electronic" and inserted "Contents of wire or electronic" in both subsec. headings, struck out "contents of an electronic" and inserted "contents of a wire or electronic" each place it appeared, and struck out "any electronic" and inserted "any wire or electronic" each place it appeared.

Pub.L. 107-56, § 220(a)(1), struck out "under the Federal Rules of Criminal Procedure" and inserted "using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation" each place appearing.

Subsec. (c)(1). Pub.L. 107-56, § 212(b)(1)(C)(i), (ii), struck out "(A) Except as provided in subparagraph (B), a provider of electronic communication service or remote computing service may" and inserted "A governmental entity may require a provider of electronic communication service or remote computing service to" and struck out "covered by subsection (a) or (b) of this section) to any person other than a governmental entity.

"**(B)** A provider of electronic communication service or remote computing service shall disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) to a governmental entity" following "(not including the contents of communications" and inserted a closing parenthesis.

Subsec. (c)(1)(A). Pub.L. 107-56, § 220(a)(1), struck out "under the Federal Rules of Criminal Procedure" and inserted "using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation" each place appearing.

Subsec. (c)(1)(C), (c)(2). Pub.L. 107-56, § 212(b)(1)(C)(iii), designated former subpar. (C) of par. (1) as par. (2) of subsec. (c).

Subsec. (c)(1)(B)(i) to (iv), (c)(1)(A) to (D). Pub.L. 107-56, § 212(b)(1)(C)(iv), designated former clauses (i) to (iv) of subsec. (c)(1)(B) as subpars. (A) to (D) of subsec. (c)(1).

Subsec. (c)(1)(D). Pub.L. 107-56, § 212(b)(1)(C)(v), struck out the period and added "; and".

Subsec. (c)(1)(E). Pub.L. 107-56, § 212(b)(1)(C)(vi), added subpar. (E).

Subsec. (c)(2), (3). Pub.L. 107-56, § 212(b)(1)(B), designated par. (2) as par. (3).

Subsec. (c)(2). Pub.L. 107-56, § 210, struck out "entity the name, address, local and long distance telephone toll billed records, telephone number or other subscriber number or identity, and length of service of a subscriber" and inserted: "entity the--

"**(A)** name;

"**(B)** address;

"**(C)** local and long distance telephone connection records, or records of session times and durations;

"**(D)** length of service (included start date) and types of service utilized;

"**(E)** telephone or instrument number or other subscriber number or identity, included any temporarily assigned network address; and

"**(F)** means and source of payment for such service (included any credit card or bank account number),

of a subscriber" and struck out "and the types of services the subscriber or customer utilized," preceding "when the governmental entity uses an administrative subpoena".

Subsec. (c)(2). Pub.L. 107-56, § 212(b)(1)(D), struck out "subparagraph (B)" and inserted "paragraph (1)".

Subsec. (d). Pub.L. 107-56, § 220(b), struck out "described in section 3127(2)(A)" after "competent jurisdiction".

1998 Amendments. Subsec. (c)(1)(B)(ii). Pub.L. 105-184, § 8(1), struck out "or" at the end of clause (ii).

Subsec. (c)(1)(B)(iii). Pub.L. 105-184, § 8(2), struck out the period at the end of clause (iii) and inserted "; or".

Subsec. (c)(1)(B)((iv). Pub.L. 105-184, § 8(3) added clause (iv).

1996 Amendments. Subsec. (c)(1)(C). Pub.L. 104-293 inserted "local and long distance" after "address,".

Subsec. (d). Pub.L. 104-294, § 605(f), substituted "in section 3127(2)(A)" for "in section 3126(2)(A)".

Subsec. (f). Pub.L. 104-132, § 804, added subsec. (f).

1994 Amendments. Subsec. (c)(1)(B)(i) to (iii). Pub.L. 103-414, § 207(a)(1)(A), struck out former cl. (i), which related to use of subpoenas, and redesignated former cls. (ii) and (iii) as (i) and (ii), respectively. Former cl. (iv) redesignated (iii).

Subsec. (c)(1)(B)(iv). Pub.L. 103-414, § 207(a)(1)(A), redesignated former cl. (iv) as (iii).

Subsec. (c)(1)(C). Pub.L. 103-414, § 207(a)(1)(B), added subpar. (C).

Subsec. (d). Pub.L. 103-414, § 207(a)(2), substituted provisions directing that a court order issued by a court of competent jurisdiction described in section 3126(2)(A) shall issue only if the governmental entity offers specific and articulable facts showing reasonable grounds to believe that the wire or electronic communications sought are relevant and material to an ongoing criminal investigation for former provisions which had provided that such court order would issue only if the governmental entity showed that there was reason to believe that the wire or electronic communications sought were relevant to a legitimate law enforcement inquiry.

Pub.L. 103-322, § 330003(b), substituted "section 3127(2)(A)" for "section 3126(2)(A)" in existing provisions.

1988 Amendments. Subsec. (b)(1)(B)(i). Pub.L. 100-690, § 7038, added "or trial" following "State grand jury".

Subsec. (c)(1)(B)(i). Pub.L. 100-690, § 7038, added "or trial" following "State grand jury".

Subsec. (d). Pub.L. 100-690, § 7039, added "may be issued by any court that is a court of competent jurisdiction set forth in section 3126(2)(A) of this title and" following "of this section".

Effective and Applicability Provisions

2002 Acts. Amendment to this section by Pub.L. 107-296 effective 60 days after Nov. 25, 2002, see Pub.L. 107-296, § 4, set out as a note under 6 U.S.C.A. § 101.

1986 Acts. Section effective 90 days after Oct. 21, 1986 except as otherwise provided in section 202 of Pub.L. 99-508 with respect to conduct pursuant to court order or extension, see section 202 of Pub.L. 99-508, set out as a note under

RIF

section 2701 of this title.

Sunset Provisions

Provision that amendments by Pub.L. 107-56, Title II, Oct. 26, 2001, 115 Stat. 278, with certain exclusions, shall cease to have effect on March 10, 2006, except with respect to any particular foreign intelligence investigation that began before that date, or with respect to any particular offense or potential offense that began or occurred before that, such provisions to continue in effect, was repealed by Pub.L. 109-177, § 102(a), see Pub.L. 107-56, § 224, as amended, set out as a note under 18 U.S.C.A. § 2510.

LAW REVIEW COMMENTARIES

1994 Digital Telephone Act: A response to technology. Peter A. Crusco and Roseanna DeMaria, 213 N.Y.L.J. 1 (April 19, 1995).

Can police track your wireless calls? Call location information and privacy law. Laurie Thomas Lee, 21 Cardozo Arts & Ent. L.J. 381 (2003).

Cyberslapp suits and John Doe subpoenas: balancing anonymity and accountability in cyberspace. Shaun B. Spencer, 19 J.Marshall J. Computer & Info.L. 493 (2001).

Internet surveillance law after the USA Patriot Act: The big brother that isn't. Orin S. Kerr, 97 Nw. U. L. Rev. 607 (2003).

Keeping "private e-mail" private: A proposal to modify the Electronic Communications Privacy Act. Robert S. Steere, 33 Val. U.L.Rev. 231 (1998).

The states and the electronic communications privacy act: The need for legal processes that keep up with the times. Monique Mattei Ferraro, 22 J. Marshall J. Computer & Info. L. 695 (2004).

LIBRARY REFERENCES

American Digest System

Telecommunications 491.

Key Number System Topic No. 372.

Corpus Juris Secundum

CJS Telecommunications § 240, Stored Communications and Transactional Records Access.

RESEARCH REFERENCES

ALR Library

37 ALR, Fed. 2nd Series 323, Allowable Use of Federal Pen Register and Trap and Trace Device to Track Post-Cut-Through Dialed Digits (PCTDD).

RJF

25 ALR, Fed. 2nd Series 323, Construction and Application of Communications Assistance for Law Enforcement Act (CALEA), 47 U.S.C.A. §§ 1001 to 1010.

15 ALR, Fed. 2nd Series 537, Allowable Use of Federal Pen Register and Trap and Trace Device to Trace Cell Phones and Internet Use.

61 ALR, Fed. 7, Defense of Good Faith in Action for Damages Against Law Enforcement Official Under 42 U.S.C.A. § 1983, Providing for Liability of Person Who, Under Color of Law, Subjects Another to Deprivation Of...

92 ALR 5th 15, Expectation of Privacy in Internet Communications.

84 ALR 5th 1, Validity of Search or Seizure of Computer, Computer Disk, or Computer Peripheral Equipment.

134 ALR 614, Admissibility of Evidence Obtained by Government or Other Public Officer by Intercepting Letter or Telegraph or Telephone Message.

Encyclopedias

2 Am. Jur. Proof of Facts 2d 545, Reliability of Scientific Devices--Telephone Calling Line Identification.

41 Am. Jur. Proof of Facts 3d 1, Recovery and Reconstruction of Electronic Mail as Evidence.

67 Am. Jur. Proof of Facts 3d 249, Proof of Liability for Violation of Privacy of Internet User, by Cookies or Other Means.

86 Am. Jur. Proof of Facts 3d 217, Use of Call Detail Record Evidence in Telecommunications "Phantom Traffic" and Other Litigation.

100 Am. Jur. Proof of Facts 3d 89, Proof of Instant Message, Blog, or Chat as Evidence.

113 Am. Jur. Proof of Facts 3d 1, Password-Protected Electronic Evidence in Criminal Actions.

97 Am. Jur. Trials 1, Telecommunications and Other Litigation: Call Detail Records and Fraud.

103 Am. Jur. Trials 123, Admission of E-Mail Evidence in Civil Actions.

Am. Jur. 2d Banks § 635, Giving Information or Advice to Depositors or Others.

Am. Jur. 2d Computers and the Internet § 9, Disclosure by Remote Computing Service of Wire or Electronic Communications or Records; Voluntary Disclosure; Backup Preservation of Communications--Required Disclosure of Communications or Records.

Am. Jur. 2d Computers and the Internet § 22, Expectation of Privacy in Computer Files and Internet Communications; Effect Thereof.

Am. Jur. 2d Computers and the Internet § 74, Disclosure of Wire or Electronic Communications or Records.

RIF

Am. Jur. 2d Telecommunications § 187.5, Stored Wire and Electronic Communications, Generally; Required Disclosure.

Forms

5A West's Federal Forms § 8564, Computer Searches.

5A West's Federal Forms § 8594, Order Granting Government Request for a Pen Register.

Treatises and Practice Aids

Federal Procedure, Lawyers Edition § 22:322, Obtaining Contents of Wire or Electronic Communications in Electronic Storage.

Federal Procedure, Lawyers Edition § 22:323, Electronic Communications in Remote Computing Service.

Federal Procedure, Lawyers Edition § 22:324, Records Concerning Electronic-Communication Service or Remote Computing Service.

Federal Procedure, Lawyers Edition § 22:325, Court Order.

Federal Procedure, Lawyers Edition § 22:326, Preservation of Records and Evidence.

Federal Procedure, Lawyers Edition § 22:328, Delayed Notice.

Federal Procedure, Lawyers Edition § 72:816, Wrongful Access to Stored Electronic Communication.

Wright & Miller: Federal Prac. & Proc. § 661, Overview.

NOTES OF DECISIONS

RIF

1/2. Constitutionality

Fourth Amendment required government to obtain a warrant, based on a showing of probable cause on oath or affirmation, in order to obtain an order, pursuant to the Stored Communications Act (SCA), directing a provider of electronic communication services to disclose cell-cite information for a certain mobile telephone during a past 58-day period, despite its allegation that specific and articulable facts existed showing that there were reasonable grounds to believe that the information sought was relevant and material to an ongoing criminal investigation. In re Application of U.S. for an order authorizing release of historical cell-cite information, E.D.N.Y.2010, 2010 WL 3463132. Telecommunications 1475

1. Toll billing records

For purposes of provision of Electronic Communications Privacy Act as amended by Communications Assistance for Law Enforcement Act, which authorizes grand jury to obtain from electronic communication service provider by subpoena telephone toll billing records, term "telephone toll billing records" covers all records maintained of individual calls made from particular telephone number or attributed to it that are or could be subject of particularized charge depending on billing plan offered by provider and accepted by customer; in other words, "telephone toll billing record" is broad enough to cover all records of calls from or attributed to particular number, regardless of whether, in fact, separate charge is assessed for each call. Matter of Grand Jury Subpoenas to Southwestern Bell Mobile Systems, Inc., W.D.Mo.1995, 894 F.Supp. 355. Grand Jury 36.4(1)

2. Warrant

If government makes requisite showing, under the Stored Communications Act (SCA), of specific and articulable facts establishing 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, the court has discretion to require a warrant prior to ordering a cell phone provider to produce a customer's historical cellular tower data, also known as cell site location information (CSLI). In re Application of U.S. for An Order Directing a Provider of Electronic Communication Service to Disclose Records to Government, C.A.3 (Pa.) 2010, 2010 WL 3465170. Telecommunications 1475

Bank's alleged disclosure of contents of electronic funds transfers in electronic storage, on same day funds were transferred to customer's account, would not be permitted by Electronic Communication Privacy Act (ECPA), if disclosures were pursuant to "verbal instructions," instead of warrant. Lopez v. First Union Nat. Bank of Florida, C.A.11 (Fla.) 1997, 129 F.3d 1186, rehearing and suggestion for rehearing en banc denied 141 F.3d 1191. Telecommunications 1436

Government was not required to serve notice of search warrant to subscribers who sent or received e-mails, which warrant was served on internet service providers (ISPs) for electronic information stored on providers' servers, since e-mails to be seized were in possession of ISPs. In re U.S., D.Or.2009, 665 F.Supp.2d 1210. Telecommunications 1477

Under Stored Wire and Electronic Communications and Transactional Records Access Act, previously opened e-mails stored by Internet service provider (ISP) for users of "web-based" e-mail account which were less than 181 days old were not in electronic storage, but instead were held or maintained solely to provide the customer storage or computer processing services, and thus government could obtain e-mails from ISP using a trial subpoena, rather than a warrant; under the default method of using the account, users accessed their e-mail over the web from any computer, rather than automatically downloading their messages to their own computers as with non-web-based e-mail service. U.S. v. Weaver, C.D.Ill.2009, 636 F.Supp.2d 769. Telecommunications 1463; Witnesses 16

Government was not entitled to disclosure from telecommunications provider of historical cell site information upon showing under Stored Communications Act (SCA) of specific and articulable facts that information was relevant to ongoing criminal investigation, but was required to demonstrate probable cause; historical cell site information may provide de facto "real-time" physical location of cell phone, such that its use is tantamount to a tracking device. In re Applications of the U.S. for Orders Pursuant to Title 18, U.S. Code, Section 2703(d) to Disclose Subscriber Information and Historical Cell Site Information for Mobile Identification Numbers: (XXX)XXX-AAAA, (XXX)XXX-BBBB, (XXX)XXX-CCCC, D.Mass.2007, 509 F.Supp.2d 64, reversed 509 F.Supp.2d 76. Telecommunications 1485

Government was entitled to order authorizing use of a pen register and trap-and-trace device and release of subscriber and other information, including cell-site information, where authorization sought was limited to provision of cell-site information at the origin and termination of calls and during the progress of calls not initiated by the government itself, and did not extend to information that could be used to track the location of the phone. In re U.S. for an Order, S.D.Tex.2006, 433 F.Supp.2d 804. Telecommunications 1475

Government was not entitled to release of prospective "cell site data" that would disclose the location of the person using a particular cell phone, absent any showing of probable cause that the information or materials to be seized were evidence of a crime, contraband, fruits of crime, or other items illegally possessed, or property designed for use or intended for use in committing a crime; government's tautological statement that there was probable cause to believe that the information would be relevant to an ongoing criminal investigation was unavailing to supply the requisite showing. In re Application of U.S. for an Order Authorizing the Release of Prospective Cell Site Information, D.D.C.2005, 407 F.Supp.2d 132, subsequent determination 407 F.Supp.2d 134. Telecommunications 1438

In seeking to obtain prospective or "real-time" cell site data, which reveals user's physical location when cellular telephone is turned on, government does not seek to intercept contents of telephone user's communication, and therefore government cannot obtain cell site data pursuant to wiretap statute or provisions of Stored Communications Act (SCA) authorizing disclosure of contents of stored communications. In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority, S.D.Tex.2005, 396 F.Supp.2d 747. Telecommunications 1438

Cell site location information, revealing general geographic location of subject cellular telephone, was not "the contents of an electronic communication" that could be obtained by government under the Electronic Communications Privacy Act during a criminal investigation without showing of probable cause; disclosure of such information would have effectively allowed the installation of a tracking device without the showing of probable cause normally required for a warrant. In re Authorizing the Use of a Pen Register, E.D.N.Y.2005, 384 F.Supp.2d 562, on reconsideration 396 F.Supp.2d 294. Telecommunications 1475

Fact that defendant was arrested in Florida on Indiana warrant for possession of child pornography did not prohibit federal agents from investigating violation of federal law arising from possession of child pornography in Florida at time of his arrest on out-of-state charges, and thus district court in Florida was authorized to issue warrant for seizure of electronic data regarding defendant's internet viewing activities. In re Search Warrant, M.D.Fla.2003, 362 F.Supp.2d 1298, reversed 2005 WL 3844032. Obscenity 7.6

Accused did not have a reasonable expectation of privacy in subscriber information he provided to commercial internet site, and thus special agent's obtaining of such information without a warrant from company which operated site did not violate the Fourth Amendment; subscriber information was not treated as confidential, subscriber agreement put subscriber on notice that the information could be disclosed to third parties, and reasonable subscriber could conclude from provisions of the Electronic Communications Privacy Act (ECPA) that subscriber information was not protected from third-party disclosure. U.S. v. Ohnesorge, 60 M.J. 946 (N.M.Ct.Crim.App. 2005). Military Justice

RIF

1080; Searches And Seizures 26

Prison's disclosure to United States Attorney's Office prisoner's telephone records during his incarceration while awaiting trial on narcotics and money laundering charges was shielded by Stored Communications Act exceptions allowing disclosure for records concerning electronic communication service upon obtaining warrant. Thomas v. Seth, C.A.3 (Pa.) 2009, 317 Fed.Appx. 279, 2009 WL 692374, Unreported. Prisons 340; Telecommunications 1437

2a. Expectation of privacy

Defendant had no expectation of privacy, under Fourth Amendment, in government's acquisition of his subscriber information, including internet protocol (IP) address and name, from third-party service providers, pursuant to Electronic Communications Privacy Act (ECPA) and Pennsylvania law, authorizing such disclosure upon specific and articulable facts showing reasonable grounds to believe records were relevant and material to ongoing criminal investigation, as would support issuing search warrant that resulted in seizure of defendant's computer with thousands of images of child pornography; where defendant voluntarily transmitted such information to internet providers and enabled peer-to-peer file sharing on computer, which allowed anyone with internet access ability to enter his computer and access certain folders. U.S. v. Perrine, C.A.10 (Kan.) 2008, 518 F.3d 1196, appeal from denial of post-conviction relief dismissed 2010 WL 1225810. Obscenity 7.6; Telecommunications 1335

2b. Sufficiency of affidavits to support disclosure of IP address and name

Government's affidavits contained specific and articulable facts showing reasonable grounds to believe information sought from defendant was relevant and material to ongoing criminal investigation, as required for applications for court orders to disclose defendant's internet protocol (IP) address and name, pursuant to Electronic Communications Privacy Act (ECPA) and Pennsylvania law, authorizing disclosure of electronic communications and transaction records by third-party service providers, thereby supporting issuance of search warrant that resulted in seizure of defendant's computer with thousands of images of child pornography; affidavits indicated that informant immediately contacted police, which suggested he was simply concerned citizen, that officer had personally read defendant's chat log, and that every login but one matched defendant's IP address. U.S. v. Perrine, C.A.10 (Kan.) 2008, 518 F.3d 1196, appeal from denial of post-conviction relief dismissed 2010 WL 1225810. Obscenity 7.6; Telecommunications 1335

2c. Suppression of evidence

Although discrepancies in detective's testimony were indicative of less-than-exemplary detective work and unfavorable to government, at suppression hearing for defendant charged with conspiracy to distribute controlled substances, detective's missteps in his written documentation and testimony were merely minor mistakes, precluding suppression of evidence from government's legal interceptions of telephone communications by pen register and trap and trace device, recording numerical data of ingoing and outgoing telephone numbers to identify co-defendant's new telephone number, that resulted in authorization to wiretap conversations leading to defendant's indictment. U.S. v. Terry, C.A.7 (Wis.) 2009, 572 F.3d 430. Criminal Law 394.3

Suppression of evidence is not available to remedy violations of Electronic Communications Privacy Act (ECPA) and Pennsylvania law, authorizing government to require disclosure of stored electronic communications and transaction records by third-party service providers upon specific and articulable facts showing reasonable grounds to believe records are relevant and material to ongoing criminal investigation. U.S. v. Perrine, C.A.10 (Kan.) 2008, 518 F.3d 1196, appeal from denial of post-conviction relief dismissed 2010 WL 1225810. Criminal Law 394.3

3. Civil actions

Electronic Communications Privacy Act does not authorize civil suit against governmental entity for "violation" of section prohibiting providers of electronic communication services and remote computing services from improperly disclosing information to governmental entity; particular statute does not authorize civil suits against governmental entities for improperly obtaining customer records. Tucker v. Waddell, C.A.4 (N.C.) 1996, 83 F.3d 688. Telecommunications 1443

Electronic Communications Privacy Act prohibited Internet service provider from producing the emails of non-party witnesses in an action pending in another district, which were sought pursuant to a subpoena duces tecum; issuance of the civil discovery subpoena was not an exception to the provisions of the Act so as to allow the provider to disclose the communications. In re Subpoena Duces Tecum to AOL, LLC, E.D.Va.2008, 550 F.Supp.2d 606. Witnesses 16

Purported common law immunity accorded telecommunications providers for cooperating with government officials conducting surveillance activities did not bar action against provider that allegedly participated in warrantless surveillance program; common law immunity appeared to overlap considerably with protections afforded under subsequently enacted statutory certification provision, and there was no reason to presume that such immunity was available simply because Congress has not expressed a contrary intent. Hepting v. AT & T Corp., N.D.Cal.2006, 439 F.Supp.2d 974, remanded 539 F.3d 1157. Telecommunications 1441

District attorney's office was "governmental entity," for purposes of provision of Electronic Communications Privacy Act (ECPA) requiring governmental entities to reimburse telecommunications service providers for costs of complying with subpoenas for electronic records, despite district attorney's contention that provision only applied to federal entities, where ECPA made no such distinction. Ameritech Corp. v. McCann, E.D.Wis.2004, 308 F.Supp.2d 911, vacated 403 F.3d 908, rehearing and rehearing en banc denied , on remand 2005 WL 1398606. Telecommunications 1452

Two police officers who obtained plaintiff's subscriber information from Internet service provider (ISP) using invalid search warrant were liable for violation of Electronic Communication Privacy Act (ECPA); request for information sent to ISP by officers had substantial resemblance to compulsory court order, and officers clearly intended that ISP supply information they sought, there was no "emergency" under ECPA, and subscriber did not consent to disclosure. Freedman v. America Online, Inc., D.Conn.2004, 303 F.Supp.2d 121. Telecommunications 1440; Telecommunications 1441

Term "trial subpoena" in section of the Electronic Communications Privacy Act (ECPA) requiring a provider of electronic communication to disclose customer information to a government entity only in response to "an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena" does not encompass a discovery subpoena duces tecum issued under rule governing subpoenas. F.T.C. v. Netscape Communications Corp., N.D.Cal.2000, 196 F.R.D. 559. Witnesses 16

4. Good faith

Secret Service agents' seizure, pursuant to search warrant, of computers, disks, and other materials containing electronic communications stored in computer bulletin board respecting operator of bulletin board and other users of bulletin board from operator's premises constituted violation of Stored Wire and Electronic Communications and Transactional Records Access Act, despite government's contention that Secret Service had "good faith" reliance on search warrant. Steve Jackson Games, Inc. v. U.S. Secret Service, W.D.Tex.1993, 816 F.Supp. 432, affirmed 36 F.3d 457. Telecommunications 1439

5. Damages

District court would assess statutory damages of $1,000 for each plaintiff against government and Secret Service as result of violation of Stored Wire and Electronic Communications and Transactional Records Access Act through Secret Service agents' seizure, pursuant to search warrant, of computers, disks, and other materials containing electronic communications stored in computer bulletin board respecting plaintiffs operator of bulletin board and other users of bulletin board from operator's premises. Steve Jackson Games, Inc. v. U.S. Secret Service, W.D.Tex.1993, 816 F.Supp. 432, affirmed 36 F.3d 457. Searches And Seizures 85

6. Cell site information

Under the Stored Communications Act (SCA), to obtain order compelling cell phone provider to produce customer's historical cellular tower data, also known as cell site location information (CSLI), government had burden to show specific and articulable facts establishing reasonable grounds that customer's CSLI was relevant and material to an ongoing criminal investigation, which was a lesser burden than establishing probable cause. In re Application of U.S. for An Order Directing a Provider of Electronic Communication Service to Disclose Records to Government, C.A.3 (Pa.) 2010, 2010 WL 3465170. Telecommunications 1475

Stored Communications Act, either alone or in tandem with Pen Registry Statute, does not authorize access to individual's cellular phone-derived location information, either past or prospective, on simple showing of articulable relevance to ongoing investigation rather than probable cause. In re U.S. for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government, W.D.Pa.2008, 534 F.Supp.2d 585, affirmed 2008 WL 4191511. Telecommunications 1475

Historical cell site information held by cell phone service provider was not "content information" and thus was obtainable under the "specific and articulable facts" standard of the Stored Communications Act (SCA); information sought, which concerned the location of a cell tower in relation to the point of origin (or termination) of calls, disclosed nothing about the substance of the calls. In re Applications of U.S. for Orders Pursuant to Title 18, U.S.Code Section 2703(d), D.Mass.2007, 509 F.Supp.2d 76. Telecommunications 1475

Use of term "solely" in section of Communications Assistance for Law Enforcement Act (CALEA) which forbids providers from disclosing "any information that may disclose the physical location of the subscriber" when government proceeds "solely" pursuant to authority for pen registers and trap and trace devices, does not permit government to combine pen/trap statute with Stored Communications Act, which permits recovery of historical information upon showing of specific and articulable facts, to obtain cell site information without showing of probable cause. In re Applications of the U.S. for Orders Pursuant to Title 18, U.S. Code, Section 2703(d) to Disclose Subscriber Information and Historical Cell Site Information for Mobile Identification Numbers: (XXX)XXX-AAAA, (XXX)XXX-BBBB, (XXX)XXX-CCCC, D.Mass.2007, 509 F.Supp.2d 64, reversed 509 F.Supp.2d 76. Telecommunications 1475

Secured Communications Act (SCA) could not be combined with the procedural safeguards of the Pen Register Statute to authorize government's acquisition of prospective cell phone site information from pen register and trap and trace devices; SCA contemplated orders for stored rather than prospective information and contained specific prohibition against disclosure of customer records to the government, the exceptions to the prohibition did not include pen register and trap and trace orders, SCA did not encompass cell phone location data, and cell site information was not an "electronic communication" under SCA. In re Application of U.S. for Order, D.Puerto Rico 2007, 497 F.Supp.2d 301. Telecommunications 1475

Limited cell site information could not be obtained prospectively by government under the dual or hybrid authority of

the Pen/Trap Statute and the Stored Communications Act (SCA). In re U.S., S.D.Tex.2006, 441 F.Supp.2d 816. Telecommunications 1475

Government was not entitled to order compelling cellular telephone company to provide real-time cell site data for particular phone, on less than probable cause, on theory that convergence of Pen Register and Trap and Trace Statute, exception clause of Communications Assistance for Law Enforcement Act (CALEA), and Stored Communications Act (SCA) authorized it; convergence was not provided for in plain language of statutes in question. In re U.S. for an Order Authorizing Installation and Use of a Pen Register, W.D.N.Y.2006, 415 F.Supp.2d 211. Telecommunications 1475

Government was not entitled to order requiring cell phone company to provide prospective cell site information, namely the locations of cell towers being used at commencement and termination of calls to and from a particular cell phone, absent any authority other than the Pen/Trap Statute in combination with the Stored Communications Act (SCA); information constituted call-identifying information within meaning of the Communications Assistance to Law Enforcement Act (CALEA), which barred use of pen registers and trap devices to obtain information that might disclose a cell phone subscriber's physical location. In re U.S. For an Order Authorizing the Disclosure of Prospective Cell Site Information, E.D.Wis.2006, 412 F.Supp.2d 947, affirmed 2006 WL 2871743. Telecommunications 1475

Under Pen Register Statute in combination with Stored Communications Act (SCA), Government was entitled to order authorizing use of a pen register and trap and trace device on a number assigned to a cell phone, and disclosure of prospective cell site information; application set forth specific and articulable facts demonstrating reasonable grounds to believe that the information sought was relevant and material to an ongoing criminal investigation. In Matter of Application of U.S. For an Order, W.D.La.2006, 411 F.Supp.2d 678. Telecommunications 1475

7. Review

Claims in which criminal suspect sought relief against future seizures of his e-mails were ripe for review, despite government's contention that he could not prove that future seizures would occur, given that suspect had suffered past alleged violations of his Fourth Amendment rights due to same conduct that he sought to have enjoined, that continued threat of injury existed due to ongoing nature of investigation against suspect, that government's ex parte approach to obtaining suspect's e-mails under Stored Communications Act (SCA) precluded possibility of judicial review at subsequent and more appropriate time, and that past seizures presented adequate factual basis on which to assess government's conduct. Warshak v. U.S., C.A.6 (Ohio) 2007, 490 F.3d 455, rehearing granted , opinion vacated. Federal Courts 13

8. Ripeness

Issue of whether government should be enjoined from conducting future ex parte searches of criminal suspect's e-mails pursuant to Stored Communications Act (SCA), and whether such a search would violate Fourth Amendment, was not ripe for adjudication; suspect had been indicted and convicted of various crimes, following conviction it was doubtful that government would conduct future ex parte searches of suspect's e-mails, government's interest in confidentiality of ongoing investigations no longer existed, it was unknown what type of internet service suspect would have in future and suspect would have varying expectations of privacy depending on service-provider agreement, and there was no risk of hardship to suspect if consideration was withheld. Warshak v. U.S., C.A.6 (Ohio) 2008, 532 F.3d 521. Telecommunications 1451

9. Pen register and trap and trace devices

Government was entitled to order authorizing use of a pen register and trap-and-trace device and release of subscriber

and other information, including cell-site information, where authorization sought was limited to provision of cell-site information at the origin and termination of calls and during the progress of calls not initiated by the government itself, and did not extend to information that could be used to track the location of the phone. In re U.S., S.D.Tex.2007, 622 F.Supp.2d 411. Telecommunications 1475

10. Post-cut through dialed digits

Government could not obtain "post-cut-through dialed digits" containing communication contents under the authority of the Pen/Trap Statute. In re U.S., S.D.Tex.2007, 622 F.Supp.2d 411. Telecommunications 1475

11. Construction, generally

USA Patriot Act amendments to Stored Communications Act provision regarding required disclosure, by internet service provider (ISP), of contents of wire or electronic communications in electronic storage incorporated procedural, but not substantive, portions of federal rule regarding supplementary and special proceedings for searches and seizure; by its definition of "procedure," provision incorporated only portions of rule that discussed "steps to be taken" or "specific method" of issuing warrant, interpretation gave meaning to change in language from broad word "under" to more narrow phrase "using the procedures described in," and word "procedures" was modified by the phrase "described in," which expressed Congress's intent that only procedural aspects of rule applied to provision. In re U.S., D.Or.2009, 665 F.Supp.2d 1210. Telecommunications 1475

12. ---- Construction with rules of criminal procedure, construction

USA Patriot Act amendments to Stored Communications Act provision regarding required disclosure, by internet service provider (ISP), of contents of wire or electronic communications in electronic storage incorporated procedural, but not substantive, portions of federal rule regarding supplementary and special proceedings for searches and seizure; by its definition of "procedure," provision incorporated only portions of rule that discussed "steps to be taken" or "specific method" of issuing warrant, interpretation gave meaning to change in language from broad word "under" to more narrow phrase "using the procedures described in," and word "procedures" was modified by the phrase "described in," which expressed Congress's intent that only procedural aspects of rule applied to provision. In re U.S., D.Or.2009, 665 F.Supp.2d 1210. Telecommunications 1475

13. Communications subject to disclosure

Webmail and private messaging services provided on social networking and website hosting websites were not subject to subpoena duces tecum under the Stored Communications Act (SCA); such messages were not readily accessible to the general public, and therefore, were inherently private. Crispin v. Christian Audigier, Inc., C.D.Cal.2010, 2010 WL 2293238. Witnesses 16

18 U.S.C.A. § 2703, 18 USCA § 2703

Current through P.L. 112-3 (excluding P.L. 111-296, 111-314, 111-320, 111-350, 111-377, and 111-383) approved 2-25-11

END OF DOCUMENT

631 F.3d 266
(Cite as: 631 F.3d 266)

H

United States Court of Appeals,
Sixth Circuit.
UNITED STATES of America, Plaintiff-Appellee,
v.
Steven **WARSHAK** (08-3997/4085; 09-3176); Harriet **Warshak** (08-3997/4087/4429); TCI Media, Inc. (08-3997/4212), Defendants-Appellants.

Nos. 08-3997, 08-4085, 08-4087, 08-4212, 08-4429, 09-3176.
Argued: June 16, 2010.
Decided and Filed: Dec. 14, 2010.

Background: Defendants, the founder and CEO of company that distributed herbal supplement purported to enhance male sexual performance, and founder's mother, who processed credit card payments, were convicted by jury of conspiracy to commit mail fraud, bank fraud, and money laundering, and were sentenced to prison and ordered to forfeit $500 million in assets. The United States District Court for the Southern District of Ohio, S. Arthur Spiegel, J., 562 F.Supp.2d 986,reconsideration denied 2008 WL 4059811, denied defendants' motions for judgment of acquittal or new trial, and to set aside forfeiture verdicts. Defendants appealed convictions, sentences, and forfeiture judgments.

Holdings: The Court of Appeals, Boggs, Circuit Judge, held that:
(1) while defendant enjoyed reasonable expectation of privacy in his e-mails vis-a-vis his Internet service provider (ISP) and government agents violated his Fourth Amendment rights by compelling ISP to turn over email without first obtaining warrant based on probable cause, because agents relied in good faith on provisions of Stored Communications Act, exclusionary rule did not apply;
(2) district court did not err in refusing to hold full-fledged *Kastigar* hearing when determining whether government agents had improperly used privileged materials seized during valid search of company's headquarters;
(3) district court did not abuse its discretion by failing to order government to provide electronic discovery in a different format;
(4) district court did not err in refusing to grant principal a new trial based on alleged *Brady* violation;
(5) district court did not err in refusing to grant defendants new trial on basis of prosecutorial misconduct;
(6) evidence was sufficient to support convictions for conspiracy to commit mail, wire and bank fraud, mail fraud, bank fraud, conspiracy to commit access-device fraud, money laundering, and conspiracy to obstruct Federal Trade Commission (FTC) proceeding;
(7) district court did not err in refusing to order government to reveal before trial whether it had conducted any additional surreptitious searches of founder's emails or communications;
(8) district court failed to provide adequate explanation of its determination that defendants should be held accountable, for sentencing purposes, for $411 million in losses, and remand for that purpose was warranted;
(9) district court did not abuse its discretion in refusing to admit certain evidence during forfeiture phase of trial; and
(10) evidence was sufficient to support proceeds-money and money-laundering forfeiture judgments against company's principal, but not money-laundering forfeiture judgment against his mother.

Convictions and forfeiture judgments affirmed in part and reversed in part; sentences vacated and remanded.

Keith, Circuit Judge, filed opinion concurring in the result.

West Headnotes

[1] Criminal Law 110 ⚿394.1(1)

110 Criminal Law
110XVII Evidence
110XVII(I) Competency in General
110k394 Evidence Wrongfully Obtained
110k394.1 In General
110k394.1(1) k. In general. Most Cited Cases

Doctrine of good-faith reliance should not be perpetual shield against consequences of constitu-

tional violations; i.e., if exclusionary rule is to have any bite, courts must, from time to time, decide whether statutorily sanctioned conduct oversteps constitutional boundaries.

[2] Telecommunications 372 1475

372 Telecommunications
372X Interception or Disclosure of Electronic Communications; Electronic Surveillance
372X(B) Authorization by Courts or Public Officers
372k1475 k. Carrier's cooperation; pen registers and tracing. Most Cited Cases

Stored Communications Act (SCA) permits governmental entity to compel service provider to disclose contents of electronic communications in certain circumstances. 18 U.S.C.A. § 2701 et seq.

[3] Searches and Seizures 349 23

349 Searches and Seizures
349I In General
349k23 k. Fourth Amendment and reasonableness in general. Most Cited Cases

Fundamental purpose of Fourth Amendment is to safeguard privacy and security of individuals against arbitrary invasions by government officials. U.S.C.A. Const.Amend. 4.

[4] Searches and Seizures 349 13.1

349 Searches and Seizures
349I In General
349k13 What Constitutes Search or Seizure
349k13.1 k. In general. Most Cited Cases

Searches and Seizures 349 26

349 Searches and Seizures
349I In General
349k25 Persons, Places and Things Protected
349k26 k. Expectation of privacy. Most Cited Cases

"Search" occurs when government infringes upon expectation of privacy that society is prepared to consider reasonable; this standard breaks down into two discrete inquiries, whether target of the investigation manifested a subjective expectation of privacy in the object of the challenged search and whether society was willing to recognize that expectation as reasonable. U.S.C.A. Const.Amend. 4.

[5] Telecommunications 372 1335

372 Telecommunications
372VIII Computer Communications
372k1335 k. Privacy in general. Most Cited Cases

Telecommunications 372 1475

372 Telecommunications
372X Interception or Disclosure of Electronic Communications; Electronic Surveillance
372X(B) Authorization by Courts or Public Officers
372k1475 k. Carrier's cooperation; pen registers and tracing. Most Cited Cases

Subscriber enjoys reasonable expectation of privacy in contents of e-mails that are stored with, or sent or received through, commercial Internet Service Provider (ISP), and government may not compel commercial ISP to turn over contents of subscriber's emails without first obtaining warrant based on probable cause. U.S.C.A. Const.Amend. 4.

[6] Criminal Law 110 394.3

110 Criminal Law
110XVII Evidence
110XVII(I) Competency in General
110k394 Evidence Wrongfully Obtained
110k394.3 k. Wiretapping or other interception. Most Cited Cases

Telecommunications 372 1475

372 Telecommunications
372X Interception or Disclosure of Electronic Communications; Electronic Surveillance
372X(B) Authorization by Courts or Public Officers
372k1475 k. Carrier's cooperation; pen registers and tracing. Most Cited Cases

Even though criminal defendant enjoyed reasonable expectation of privacy in his e-mails vis-a-vis his Internet service provider (ISP) and government agents violated his Fourth Amendment rights by compelling ISP to turn over email without first obtaining warrant based on probable cause, because agents relied in good faith on provisions of Stored Communications Act (SCA), exclusionary rule did not apply; government's violation of SCA provisions was irrelevant to issue of reasonable reliance. U.S.C.A. Const.Amend. 4; 18 U.S.C.A. §§ 2701 et seq.,2703(b, d, f).

[7] Criminal Law 110 394.5(4)

110 Criminal Law
110XVII Evidence
110XVII(I) Competency in General
110k394 Evidence Wrongfully Obtained
110k394.5 Objections to Evidence
110k394.5(4) k. Presumptions and burden of proof. Most Cited Cases

Indictment and Information 210 144.2

210 Indictment and Information
210IX Motion to Dismiss
210k144.2 k. Hearing and determination. Most Cited Cases

On motion to bar government from using evidence obtained in violation of defendants' attorney-client and work product privileges and to dismiss indictment since privileged material was used to secure it, government bore burden, at *Kastigar*-like hearing, of establishing that its case was untainted by attorney-client and work product privileged material.

[8] Criminal Law 110 394.6(5)

110 Criminal Law
110XVII Evidence
110XVII(I) Competency in General
110k394 Evidence Wrongfully Obtained
110k394.6 Motions Challenging Admissibility of Evidence
110k394.6(5) k. Hearing and determination. Most Cited Cases

In criminal prosecution of founder and CEO of company that distributed herbal supplement purported to enhance male sexual performance, district court did not err in refusing to hold full-fledged *Kastigar* hearing when determining whether government agents had improperly used privileged materials seized during valid search of company's headquarters; absent compelled testimony, full protections of *Kastigar* were inapplicable, and privileged materials were not obtained as result of compelled testimony but instead were garnered pursuant to subpoena, court order, and search warrant. U.S.C.A. Const.Amend. 4.

[9] Criminal Law 110 1148

110 Criminal Law
110XXIV Review
110XXIV(N) Discretion of Lower Court
110k1148 k. Preliminary proceedings. Most Cited Cases

District court's decision on discovery matter is reviewed for abuse of discretion.

[10] Criminal Law 110 627.5(1)

110 Criminal Law
110XX Trial
110XX(A) Preliminary Proceedings
110k627.5 Discovery Prior to and Incident to Trial
110k627.5(1) k. In general; examination of victim or witness. Most Cited Cases

Federal rule which governs discovery in criminal cases is entirely silent on issue of form that discovery must take. Fed.Rules Cr.Proc.Rule 16, 18 U.S.C.A.

[11] Criminal Law 110 627.6(3)

110 Criminal Law
110XX Trial
110XX(A) Preliminary Proceedings
110k627.5 Discovery Prior to and Incident to Trial
110k627.6 Information or Things, Disclosure of
110k627.6(3) k. Particular documents or tangible objects. Most Cited Cases

In criminal prosecution of founder and CEO of company that distributed herbal supplement purported to enhance male sexual performance, and his mother, district court did not abuse its discretion by failing to order government to provide electronic discovery in different format; overwhelming majority of discovery at issue was taken directly from company's computers, which meant defendants had ready access to that information and documents were kept in the usual course of business, there was reason to believe defendants were experiencing little difficulty in accessing contents of the electronic discovery, and government provided defense with something of a guide to the electronic discovery. Fed.Rules Civ.Proc.Rule 34(b)(2)(E)(i), 28 U.S.C.A.

[12] Criminal Law 110 1991

110 Criminal Law
110XXXI Counsel
110XXXI(D) Duties and Obligations of Prosecuting Attorneys
110XXXI(D)2 Disclosure of Information
110k1991 k. Constitutional obligations regarding disclosure. Most Cited Cases

As general rule, government is under no duty to direct defendant to exculpatory evidence within larger mass of disclosed evidence.

[13] Criminal Law 110 1151

110 Criminal Law
110XXIV Review
110XXIV(N) Discretion of Lower Court
110k1151 k. Time of trial; continuance. Most Cited Cases

District court's denial of motion for continuance is reviewed for abuse of discretion.

[14] Criminal Law 110 584

110 Criminal Law
110XIX Continuance
110k583 Right of Accused to Continuance
110k584 k. In general. Most Cited Cases

Criminal Law 110 1166(7)

110 Criminal Law
110XXIV Review
110XXIV(Q) Harmless and Reversible Error
110k1166 Preliminary Proceedings
110k1166(7) k. Time for trial or hearing; continuance. Most Cited Cases

Denial of continuance requested by defendant amounts to constitutional violation only if there is an unreasoning and arbitrary insistence upon expeditiousness in the face of a justifiable request for delay; to demonstrate reversible error, defendant must show that the denial resulted in actual prejudice to his defense.

[15] Criminal Law 110 1139

110 Criminal Law
110XXIV Review
110XXIV(L) Scope of Review in General
110XXIV(L)13 Review De Novo
110k1139 k. In general. Most Cited Cases

Criminal Law 110 1156(3)

110 Criminal Law
110XXIV Review
110XXIV(N) Discretion of Lower Court
110k1156 New Trial
110k1156(3) k. Surprise and newly discovered evidence. Most Cited Cases

Court of Appeals reviews denial of motion for new trial based on *Brady* violations under abuse of discretion standard; however, district court's determination as to existence of *Brady* violation is reviewed de novo.

[16] Criminal Law 110 1991

110 Criminal Law
110XXXI Counsel
110XXXI(D) Duties and Obligations of Prosecuting Attorneys
110XXXI(D)2 Disclosure of Information
110k1991 k. Constitutional obligations regarding disclosure. Most Cited Cases

Criminal Law 110 2006

110 Criminal Law
110XXXI Counsel
110XXXI(D) Duties and Obligations of Prosecuting Attorneys
110XXXI(D)2 Disclosure of Information
110k2006 k. Request for disclosure; procedure. Most Cited Cases

To establish violation of *Brady*, defendant has burden of establishing that prosecutor suppressed evidence, that such evidence was favorable to the defense, and that the suppressed evidence was "material," i.e., there is a "reasonable probability," i.e., a probability sufficient to undermine confidence in the outcome, that, had the evidence been disclosed to the defense, the result of the proceeding would have been different.

[17] Criminal Law 110 ⚿919(1)

110 Criminal Law
110XXI Motions for New Trial
110k919 Misconduct of Counsel for Prosecution
110k919(1) k. In general. Most Cited Cases

In criminal prosecution of founder and CEO of company that distributed herbal supplement purported to enhance male sexual performance, and his mother, district court did not err in refusing to grant defendant new trial based on assertion that government had suppressed exculpatory evidence in violation of *Brady*; subject evidence was discovered post-trial while defendant was defending himself in civil action involving Federal Trade Commission (FTC) and was not material for *Brady* purposes.

[18] Criminal Law 110 ⚿1171.1(2.1)

110 Criminal Law
110XXIV Review
110XXIV(Q) Harmless and Reversible Error
110k1171 Arguments and Conduct of Counsel
110k1171.1 In General
110k1171.1(2) Statements as to Facts, Comments, and Arguments
110k1171.1(2.1) k. In general. Most Cited Cases

Criminal Law 110 ⚿2077

110 Criminal Law
110XXXI Counsel
110XXXI(F) Arguments and Statements by Counsel
110k2076 Statements as to Facts and Arguments
110k2077 k. In general. Most Cited Cases

In determining whether prosecutor's remarks and conduct merit new trial, court utilizes two-part test, first determining whether prosecutor's conduct and remarks were improper, and if so, considering and weighing four factors in determining whether impropriety was flagrant and thus warrants reversal; "flagrancy factors" are whether (1) conduct and remarks of prosecutor tended to mislead jury or prejudice defendant, (2) conduct or remarks were isolated or extensive,(3) remarks were deliberately or accidentally made, and (4) evidence against defendant was strong.

[19] Criminal Law 110 ⚿2098(1)

110 Criminal Law
110XXXI Counsel
110XXXI(F) Arguments and Statements by Counsel
110k2093 Comments on Evidence or Witnesses
110k2098 Credibility and Character of Witnesses; Bolstering
110k2098(1) k. In general. Most Cited Cases

Improper "vouching" typically occurs when prosecutor supports credibility of witness by indicating personal belief in witness's credibility, thereby placing prestige of office of the United States Attorney behind that witness.

[20] Criminal Law 110 ⚿2139

110 Criminal Law
110XXXI Counsel
110XXXI(F) Arguments and Statements by Counsel
110k2139 k. Expression of opinion as to

guilt of accused. Most Cited Cases

It is improper for prosecuting attorney in criminal case to state his personal opinion concerning guilt of defendant.

[21] Criminal Law 110 2139

110 Criminal Law
110XXXI Counsel
110XXXI(F) Arguments and Statements by Counsel
110k2139 k. Expression of opinion as to guilt of accused. Most Cited Cases

It is always improper for prosecutor to suggest that defendant is guilty merely because he is being prosecuted or has been indicted.

[22] Criminal Law 110 417(15)

110 Criminal Law
110XVII Evidence
110XVII(M) Declarations
110k416 Declarations by Third Persons
110k417 In General
110k417(15) k. Self-incriminating or exculpating declarations. Most Cited Cases

Jury may not consider guilty plea of any other person as evidence of guilt on part of defendant standing trial.

[23] Criminal Law 110 2165

110 Criminal Law
110XXXI Counsel
110XXXI(F) Arguments and Statements by Counsel
110k2164 Rebuttal Argument; Responsive Statements and Remarks
110k2165 k. In general. Most Cited Cases

Government may not advance any new contentions on rebuttal.

[24] Criminal Law 110 919(3)

110 Criminal Law
110XXI Motions for New Trial
110k919 Misconduct of Counsel for Prosecution
110k919(3) k. In argument in general. Most Cited Cases

In criminal prosecution of founder and CEO of company that distributed herbal supplement purported to enhance male sexual performance, and his mother, district court did not err in refusing to grant defendants new trial on basis of alleged prosecutorial misconduct; while some of prosecutor's remarks were improper, they were not flagrant enough to render the trial fundamentally unfair, evidence against defendants was strong, and district court offered curative instruction.

[25] Criminal Law 110 1037.1(1)

110 Criminal Law
110XXIV Review
110XXIV(E) Presentation and Reservation in Lower Court of Grounds of Review
110XXIV(E)1 In General
110k1037 Arguments and Conduct of Counsel
110k1037.1 In General
110k1037.1(1) k. Arguments and conduct in general. Most Cited Cases

Criminal Law 110 1171.1(1)

110 Criminal Law
110XXIV Review
110XXIV(Q) Harmless and Reversible Error
110k1171 Arguments and Conduct of Counsel
110k1171.1 In General
110k1171.1(1) k. Conduct of counsel in general. Most Cited Cases

Criminal Law 110 2192

110 Criminal Law
110XXXI Counsel
110XXXI(F) Arguments and Statements by Counsel
110k2191 Action of Court in Response to Comments or Conduct
110k2192 k. In general. Most Cited

Cases

Even if prosecutor's remarks are not flagrantly improper, reversal is nonetheless appropriate if three conditions are met: (1) evidence against defendants was not overwhelming, (2) defendants objected to prosecution's remarks, and (3) district court failed to issue curative instruction.

[26] Criminal Law 110 1144.13(3)

110 Criminal Law
110XXIV Review
110XXIV(M) Presumptions
110k1144 Facts or Proceedings Not Shown by Record
110k1144.13 Sufficiency of Evidence
110k1144.13(2) Construction of Evidence
110k1144.13(3) k. Construction in favor of government, state, or prosecution. Most Cited Cases

Criminal Law 110 1159.2(7)

110 Criminal Law
110XXIV Review
110XXIV(P) Verdicts
110k1159 Conclusiveness of Verdict
110k1159.2 Weight of Evidence in General
110k1159.2(7) k. Reasonable doubt. Most Cited Cases

In reviewing sufficiency of evidence to support conviction, relevant question is whether, after viewing evidence in light most favorable to prosecution, any rational trier of fact could have found essential elements of crime beyond a reasonable doubt.

[27] Criminal Law 110 1144.13(6)

110 Criminal Law
110XXIV Review
110XXIV(M) Presumptions
110k1144 Facts or Proceedings Not Shown by Record
110k1144.13 Sufficiency of Evidence
110k1144.13(6) k. Evidence considered; conflicting evidence. Most Cited Cases

Criminal Law 110 1159.2(2)

110 Criminal Law
110XXIV Review
110XXIV(P) Verdicts
110k1159 Conclusiveness of Verdict
110k1159.2 Weight of Evidence in General
110k1159.2(2) k. Verdict unsupported by evidence or contrary to evidence. Most Cited Cases

Defendant challenging sufficiency of evidence to support conviction bears very heavy burden; reviewing court will reverse judgment for insufficiency of evidence only if, viewing record as whole, judgment is not supported by substantial and competent evidence.

[28] Conspiracy 91 32

91 Conspiracy
91II Criminal Responsibility
91II(A) Offenses
91k32 k. Conspiracy to defraud in general. Most Cited Cases

Conviction for conspiracy to commit fraud requires proof beyond a reasonable doubt that defendant knowingly and willfully joined in an agreement with at least one other person to commit an act of fraud and that there was at least one overt act in furtherance of the agreement.

[29] Conspiracy 91 47(2)

91 Conspiracy
91II Criminal Responsibility
91II(B) Prosecution
91k44 Evidence
91k47 Weight and Sufficiency
91k47(2) k. Circumstantial evidence. Most Cited Cases

Circumstantial evidence that a reasonable person could interpret as showing participation in a common plan may be used to establish the existence of a conspiracy agreement.

[30] Conspiracy 91 47(1)

91 Conspiracy
91II Criminal Responsibility
91II(B) Prosecution
91k44 Evidence
91k47 Weight and Sufficiency
91k47(1) k. In general. Most Cited Cases

Conspiracy to achieve two or more unlawful goals, in the conjunctive, can properly be supported by proof of any of the alleged goals.

[31] Conspiracy 91 47(4)

91 Conspiracy
91II Criminal Responsibility
91II(B) Prosecution
91k44 Evidence
91k47 Weight and Sufficiency
91k47(3) Particular Conspiracies
91k47(4) k. Fraud and false pretenses in general. Most Cited Cases

Conspiracy 91 47(5)

91 Conspiracy
91II Criminal Responsibility
91II(B) Prosecution
91k44 Evidence
91k47 Weight and Sufficiency
91k47(3) Particular Conspiracies
91k47(5) k. Mail and wire fraud. Most Cited Cases

Evidence was sufficient to support convictions of defendant, the founder and CEO of company that distributed herbal supplement purported to enhance male sexual performance, for conspiracy to commit mail, wire and bank fraud, despite defendant's contentions that, even if government proved that conspiracy existed, its proof was insufficient to show that conspiracy lasted for entirety of period alleged in indictment, that there was no proof he entered into conspiracy to commit mail, wire, and bank fraud and all the practices that government labeled fraud were simply missteps of fledgling business attempting to find its footing while simultaneously experiencing radical growth, and that there was no conspiracy to commit bank fraud as chargeback-manipulation efforts were never intended to harm bank. 18 U.S.C.A. §§ 1341, 1344, 1349.

[32] Conspiracy 91 24.15

91 Conspiracy
91II Criminal Responsibility
91II(A) Offenses
91k23 Nature and Elements of Criminal Conspiracy in General
91k24.15 k. Duration. Most Cited Cases

Temporal scope of conspiracy is not essential or material element of charge.

[33] Conspiracy 91 47(4)

91 Conspiracy
91II Criminal Responsibility
91II(B) Prosecution
91k44 Evidence
91k47 Weight and Sufficiency
91k47(3) Particular Conspiracies
91k47(4) k. Fraud and false pretenses in general. Most Cited Cases

Conspiracy 91 47(5)

91 Conspiracy
91II Criminal Responsibility
91II(B) Prosecution
91k44 Evidence
91k47 Weight and Sufficiency
91k47(3) Particular Conspiracies
91k47(5) k. Mail and wire fraud. Most Cited Cases

Evidence was sufficient to support convictions of mother of founder and CEO of company that distributed herbal supplement purported to enhance male sexual performance for conspiracy to commit mail, wire and bank fraud; she was in charge of processing continuity shipments, and while she claimed her job amounted to little more than pushing a button and she was not made privy to any emails discussing auto-ship program or chargeback ratio, there was competent evidence in the record suggesting that she was a knowing participant in the pervasive fraud. 18 U.S.C.A. §§ 1341, 1344, 1349.

[34] Postal Service 306 35(2)

306 Postal Service
306III Offenses Against Postal Laws
306k35 Use of Mails to Defraud
306k35(2) k. Nature and elements of offense in general. Most Cited Cases

Postal Service 306 35(9)

306 Postal Service
306III Offenses Against Postal Laws
306k35 Use of Mails to Defraud
306k35(9) k. Injury from fraud. Most Cited Cases

"Mail fraud" consists of (1) scheme or artifice to defraud, (2) use of mails in furtherance of scheme, and (3) intent to deprive victim of money or property; notably, mail fraud statute does not require proof that intended victim was actually defrauded as actual success of scheme to defraud is not element of the crime. 18 U.S.C.A. § 1341.

[35] Postal Service 306 49(11)

306 Postal Service
306III Offenses Against Postal Laws
306k49 Evidence
306k49(8) Weight and Sufficiency
306k49(11) k. Use of mails to defraud. Most Cited Cases

Evidence was sufficient to support convictions of founder and CEO of company that distributed herbal supplement purported to enhance male sexual performance on 12 counts of mail fraud. 18 U.S.C.A. § 1341.

[36] Criminal Law 110 822(1)

110 Criminal Law
110XX Trial
110XX(G) Instructions: Necessity, Requisites, and Sufficiency
110k822 Construction and Effect of Charge as a Whole
110k822(1) k. In general. Most Cited Cases

Criminal Law 110 1134.51

110 Criminal Law
110XXIV Review
110XXIV(L) Scope of Review in General
110XXIV(L)4 Scope of Inquiry
110k1134.51 k. Instructions. Most Cited Cases

Court of Appeals reviews jury instruction to determine whether charge, taken as whole, fairly and adequately submits issues and applicable law to jury.

[37] Banks and Banking 52 509.10

52 Banks and Banking
52XI Federal Deposit Insurance Corporation
52k509 Offenses and Penalties
52k509.10 k. In general. Most Cited Cases

To obtain conviction for "bank fraud," government must demonstrate that (1) defendant knowingly executed or attempted to execute a scheme to defraud financial institution, (2) defendant did so with the intent to defraud, and (3) financial institution was insured by Federal Deposit Insurance Corporation (FDIC). 18 U.S.C.A. § 1344.

[38] Banks and Banking 52 509.10

52 Banks and Banking
52XI Federal Deposit Insurance Corporation
52k509 Offenses and Penalties
52k509.10 k. In general. Most Cited Cases

To have specific intent required for bank fraud, defendant need not have put bank at risk of loss in usual sense or intended to do so; rather, it is sufficient if defendant in course of committing fraud on someone causes federally insured bank to transfer funds under its possession and control. 18 U.S.C.A. § 1344.

[39] Indictment and Information 210 159(1)

210 Indictment and Information
210XI Amendment
210k158 Indictment
210k159 In General
210k159(1) k. In general. Most Cited Cases

Constructive amendments occur when indictment's terms are effectively altered by presentation of evidence and jury instructions that so modify essential elements of offense charged that there is substantial likelihood defendant was convicted of offense other than that charged in indictment.

[40] Banks and Banking 52 ⚿509.25

52 Banks and Banking
52XI Federal Deposit Insurance Corporation
52k509 Offenses and Penalties
52k509.25 k. Prosecutions. Most Cited Cases

Evidence was sufficient to support convictions of founder and CEO of company that distributed herbal supplement purported to enhance male sexual performance, and founder's mother, for bank fraud. 18 U.S.C.A. § 1344.

[41] Conspiracy 91 ⚿47(4)

91 Conspiracy
91II Criminal Responsibility
91II(B) Prosecution
91k44 Evidence
91k47 Weight and Sufficiency
91k47(3) Particular Conspiracies
91k47(4) k. Fraud and false pretenses in general. Most Cited Cases

Evidence was sufficient to support conviction of founder and CEO of company that distributed herbal supplement purported to enhance male sexual performance for conspiracy to commit access-device fraud. 18 U.S.C.A. § 1029.

[42] False Pretenses 170 ⚿7(1)

170 False Pretenses
170k3 Elements of Offenses
170k7 Nature of Pretense
170k7(1) k. In general. Most Cited Cases

Defendant need only receive requisite amount in order to violate statute prohibiting attempt to commit access-device fraud; violation does not require that defendant keep or retain payment. 18 U.S.C.A. § 1029(a)(5).

[43] United States 393 ⚿34

393 United States
393I Government in General
393k34 k. Mints, assay offices, coinage, and money. Most Cited Cases

To prove defendant guilty of "promotional money laundering," government must demonstrate that he (1) conducted financial transaction that involved proceeds of unlawful activity, (2) knew property involved was proceeds of unlawful activity, and (3) intended to promote that unlawful activity. 18 U.S.C.A. § 1956(a)(1)(A)(i).

[44] United States 393 ⚿34

393 United States
393I Government in General
393k34 k. Mints, assay offices, coinage, and money. Most Cited Cases

Evidence was sufficient to support conviction of founder and CEO of company that distributed herbal supplement purported to enhance male sexual performance for promotional money laundering. 18 U.S.C.A. § 1956(a)(1)(A)(i).

[45] United States 393 ⚿34

393 United States
393I Government in General
393k34 k. Mints, assay offices, coinage, and money. Most Cited Cases

To make out violation of "concealment money laundering" provision, government must prove three elements: (1) use of funds that are proceeds of unlawful activity, (2) knowledge that the funds are proceeds of unlawful activity, and (3) knowledge that transaction is designed in whole or in part to disguise source, ownership or control of proceeds. 18 U.S.C.A. § 1956(a)(1)(B)(i).

[46] United States 393 ⚿34

393 United States

393I Government in General
393k34 k. Mints, assay offices, coinage, and money. Most Cited Cases

Evidence was sufficient to support convictions of founder and CEO of company that distributed herbal supplement purported to enhance male sexual performance, and of media corporation, for concealment money laundering. 18 U.S.C.A. §§ 1956(a)(1)(B)(i), 1957.

[47] United States 393 ⚿34

393 United States
393I Government in General
393k34 k. Mints, assay offices, coinage, and money. Most Cited Cases

Evidence was insufficient to support conviction of mother of founder and CEO of company that distributed herbal supplement purported to enhance male sexual performance for concealment money laundering. 18 U.S.C.A. § 1956(a)(1)(B)(i).

[48] Conspiracy 91 ⚿28(3)

91 Conspiracy
91II Criminal Responsibility
91II(A) Offenses
91k28 Conspiracy to Commit Crime
91k28(3) k. Particular crimes. Most Cited Cases

Mother of founder and CEO of company that distributed herbal supplement purported to enhance male sexual performance could not be convicted of conspiracy to commit money laundering, where government failed to establish that she knew of intent behind transfer of funds between two accounts. 18 U.S.C.A. § 1956(h).

[49] Criminal Law 110 ⚿1153.1

110 Criminal Law
110XXIV Review
110XXIV(N) Discretion of Lower Court
110k1153 Reception and Admissibility of Evidence
110k1153.1 k. In general. Most Cited Cases

Criminal Law 110 ⚿1169.1(1)

110 Criminal Law
110XXIV Review
110XXIV(Q) Harmless and Reversible Error
110k1169 Admission of Evidence
110k1169.1 In General
110k1169.1(1) k. Evidence in general. Most Cited Cases

Court of Appeals reviews district court's evidentiary decisions for abuse of discretion and should only reverse when such abuse of discretion has caused more than harmless error.

[50] Criminal Law 110 ⚿470(2)

110 Criminal Law
110XVII Evidence
110XVII(R) Opinion Evidence
110k468 Subjects of Expert Testimony
110k470 Matters Directly in Issue; Ultimate Issues
110k470(2) k. Particular issues. Most Cited Cases

Criminal Law 110 ⚿474.1

110 Criminal Law
110XVII Evidence
110XVII(R) Opinion Evidence
110k468 Subjects of Expert Testimony
110k474.1 k. Intent. Most Cited Cases

Expert witness is not permitted to opine on issue of whether the defendant did or did not have mental state or condition constituting element of crime charged or of defense thereto. Fed.Rules Evid.Rule 704(b), 28 U.S.C.A.

[51] Conspiracy 91 ⚿34

91 Conspiracy
91II Criminal Responsibility
91II(A) Offenses
91k34 k. Conspiracy to obstruct or pervert justice or hinder the execution of law. Most Cited Cases

To obtain conviction for offense of conspiracy to obstruct Federal Trade Commission (FTC) proceeding, government must demonstrate three elements: (1) the existence of an agreement to violate statute prohibiting obstruction of proceedings before departments, agencies, and committees, (2) knowledge and intent to join conspiracy, and (3) an overt act constituting actual participation in conspiracy. 18 U.S.C.A. §§ 371, 1505.

[52] Obstructing Justice 282 ⚷7

282 Obstructing Justice
282k7 k. Obstructing or interfering with performance of duties of ministerial officers. Most Cited Cases

TO prove violation of statute prohibiting obstruction of proceedings before departments, agencies, and committees, government must show that (1) there was an agency proceeding, (2) defendant was aware of that proceeding, and (3) defendant intentionally endeavored corruptly to influence, obstruct or impede pending proceeding. 18 U.S.C.A. § 1505.

[53] Criminal Law 110 ⚷627.5(1)

110 Criminal Law
110XX Trial
110XX(A) Preliminary Proceedings
110k627.5 Discovery Prior to and Incident to Trial
110k627.5(1) k. In general; examination of victim or witness. Most Cited Cases

District court did not err in refusing to order government to reveal before trial whether it had conducted any additional surreptitious searches of emails or communications of defendants, the founder and CEO of company that distributed herbal supplement purported to enhance male sexual performance and his mother. Fed.Rules Cr.Proc.Rule 16, 18 U.S.C.A.

[54] Criminal Law 110 ⚷1139

110 Criminal Law
110XXIV Review
110XXIV(L) Scope of Review in General
110XXIV(L)13 Review De Novo
110k1139 k. In general. Most Cited Cases

Criminal Law 110 ⚷1158.34

110 Criminal Law
110XXIV Review
110XXIV(O) Questions of Fact and Findings
110k1158.34 k. Sentencing. Most Cited Cases

Criminal Law 110 ⚷1181.5(8)

110 Criminal Law
110XXIV Review
110XXIV(U) Determination and Disposition of Cause
110k1181.5 Remand in General; Vacation
110k1181.5(3) Remand for Determination or Reconsideration of Particular Matters
110k1181.5(8) k. Sentence. Most Cited Cases

Court of Appeals reviews district court's determination, for sentencing purposes of amount of loss attributable to defendant for clear error, whereas by contrast it reviews district court's methodology for calculating loss de novo; error with respect to loss calculation is procedural infirmity that typically requires remand. U.S.S.G. § 2B1.1(b)(1)(P), 18 U.S.C.A.

[55] Criminal Law 110 ⚷1177.3(2)

110 Criminal Law
110XXIV Review
110XXIV(Q) Harmless and Reversible Error
110k1177.3 Sentencing and Punishment
110k1177.3(2) k. Sentencing proceedings in general. Most Cited Cases

Criminal Law 110 ⚷1181.5(8)

110 Criminal Law
110XXIV Review
110XXIV(U) Determination and Disposition of Cause
110k1181.5 Remand in General; Vacation
110k1181.5(3) Remand for Determination or Reconsideration of Particular Matters

110k1181.5(8) k. Sentence. Most Cited Cases

Sentencing and Punishment 350H 996

350H Sentencing and Punishment
350HIV Sentencing Guidelines
350HIV(H) Proceedings
350HIV(H)3 Hearing
350Hk992 Findings and Statement of Reasons
350Hk996 k. Sufficiency. Most Cited Cases

In determining amount of loss from various types of fraud for sentencing purposes, district court failed to provide adequate explanation of its determination that defendants should be held accountable for $411 million in losses, and vacatur of sentence and remand for that purpose was warranted. U.S.S.G. § 2B1.1(b)(1), 18 U.S.C.A.; Fed.Rules Cr.Proc.Rule 32(i)(3)(B), 18 U.S.C.A.

[56] Criminal Law 110 1153.1

110 Criminal Law
110XXIV Review
110XXIV(N) Discretion of Lower Court
110k1153 Reception and Admissibility of Evidence
110k1153.1 k. In general. Most Cited Cases

Criminal Law 110 1153.3

110 Criminal Law
110XXIV Review
110XXIV(N) Discretion of Lower Court
110k1153 Reception and Admissibility of Evidence
110k1153.3 k. Relevance. Most Cited Cases

Court of Appeals reviews district court evidentiary rulings for abuse of discretion; broad discretion is given to district courts in determinations of admissibility based on considerations of relevance and prejudice, and those decisions will not be lightly overruled.

[57] Forfeitures 180 5

180 Forfeitures
180k5 k. Proceedings for enforcement. Most Cited Cases

Government must prove forfeiture by a preponderance of the evidence.

[58] Forfeitures 180 3

180 Forfeitures
180k3 k. Property subject to forfeiture. Most Cited Cases

To demonstrate that certain property is subject to criminal forfeiture, government must show that property constituted, or was derived from, proceeds defendant obtained directly or indirectly, as result of certain illegal conduct or conspiracy to commit certain illegal conduct or that property subject to civil forfeiture constitutes or is derived from proceeds traceable to certain illegal conduct or conspiracy to commit certain illegal conduct; notably, both statutes require forfeiture of proceeds that result from conspiracies. 18 U.S.C.A. §§ 981(a)(1)(C), 982(a)(2).

[59] Forfeitures 180 5

180 Forfeitures
180k5 k. Proceedings for enforcement. Most Cited Cases

In prosecution arising out of fraudulent sales of herbal supplement purported to enhance male sexual performance, district court did not abuse its discretion in refusing to admit certain evidence during forfeiture phase of trial; defendants attempted to introduce certain evidence which they contended would demonstrate that, from late 2003 onward, a substantial number of company's sales were legitimate, arguing that legitimacy of sales was highly relevant to issue of nexus, but government argued, and court agreed, that defendants were simply trying to relitigate issue of guilt. 18 U.S.C.A. § 982.

[60] Forfeitures 180 5

180 Forfeitures
180k5 k. Proceedings for enforcement. Most Cited

Cases

Evidence was sufficient to support proceeds-money and money-laundering forfeiture judgments against founder and CEO of company that distributed herbal supplement purported to enhance male sexual performance, but not money-laundering forfeiture judgment against founder's mother, whose convictions on money-laundering counts were improper. 18 U.S.C.A. §§ 981(a)(1)(c), 982(a)(2).

***274 ARGUED:** Martin S. Pinales, Strauss & Troy, Cincinnati, Ohio, Martin G. Weinberg, Boston, Massachusetts, for Appellants. Benjamin C. Glassman, Assistant United States Attorney, Cincinnati, Ohio, for Appellee. **ON BRIEF:** Martin S. Pinales, Candace Crouse, Strauss & Troy, Cincinnati, Ohio, Martin G. Weinberg, Boston, Massachusetts, Robert M. Goldstein, Boston, Massachusetts, for Appellants. Anne L. Porter, Assistant United States Attorney, Cincinnati, Ohio, for Appellee. Kevin S. Bankston, Electronic Frontier Foundation, San Francisco, California, for Amici Curiae.

Before: KEITH, BOGGS, and McKEAGUE, Circuit Judges.

BOGGS, J., delivered the opinion of the court, in which McKEAGUE, J., joined. KEITH, J. (pp. 333-36), delivered a separate opinion concurring in the result.

OPINION

BOGGS, Circuit Judge.

Berkeley Premium Nutraceuticals, Inc., was an incredibly profitable company that served as the distributor of Enzyte, an herbal supplement purported to enhance male sexual performance. In this appeal, defendants Steven **Warshak** ("**Warshak**"), Harriet **Warshak** ("Harriet"), and TCI Media, Inc. ("TCI"), challenge their convictions stemming from a massive scheme to defraud Berkeley's customers. **Warshak** and Harriet also challenge their sentences, as well as two forfeiture judgments.

Given the volume and complexity of the issues presented, we provide the following summary of our holdings:

(1) **Warshak** enjoyed a reasonable expectation of privacy in his emails vis-a-vis NuVox, his Internet Service Provider. *See Katz v. United States*, 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967). Thus, government agents violated his Fourth Amendment rights by compelling NuVox to turn over the emails without first obtaining a warrant based on probable cause. However, because the agents relied in good faith on provisions of the Stored Communications Act, the exclusionary rule does not apply in this instance. *See Illinois v. Krull*, 480 U.S. 340, 107 S.Ct. 1160, 94 L.Ed.2d 364 (1987).

(2) The district court did not err in refusing to hold a full-fledged hearing under *Kastigar v. United States*, 406 U.S. 441, 92 S.Ct. 1653, 32 L.Ed.2d 212 (1972), when determining whether government agents had improperly used privileged materials seized during a valid search of Berkeley's headquarters. *Kastigar* does not apply with full force outside the context of compelled testimony. *See United States v. Squillacote*, 221 F.3d 542 (4th Cir.2000).

(3) The district court did not abuse its discretion by failing to order the government to provide discovery in a different format, as Federal Rule of Criminal Procedure 16 is silent on the issue of the form that discovery must take. Moreover, the government did not duck its obligations under *Brady v. Maryland*, 373 U.S. 83, 83 S.Ct. 1194, 10 L.Ed.2d 215 (1963), by providing the defendants with massive quantities of discovery. *See United States v. Skilling*, 554 F.3d 529 (5th Cir.2009), *vacated in part on other grounds*, --- U.S. ----, 130 S.Ct. 2896, 177 L.Ed.2d 619 (2010). Finally, the district court did not err in refusing to grant the defendants a continuance so that they could continue examining the discovery materials turned over by the government.

(4) The district court did not err in refusing to grant **Warshak** a new trial based on an alleged *Brady* violation, as the purportedly exculpatory material did not rise ***275** to the level of materiality. *See Kyles v. Whitley*, 514 U.S. 419, 115 S.Ct. 1555, 131 L.Ed.2d 490 (1995).

(5) The district court did not err in refusing to grant the defendants a new trial on the basis of prosecutorial misconduct. Though the prosecution did make a number of improper remarks during its rebuttal argument, the remarks were not flagrant. *See United States v. Carter*, 236 F.3d 777 (6th Cir.2001).

(6) The evidence was sufficient to support **Warshak's** and Harriet's respective convictions for conspiracy to commit mail, wire, and bank fraud, in violation of 18 U.S.C. § 1349. *See Jackson v. Virginia,* 443 U.S. 307, 99 S.Ct. 2781, 61 L.Ed.2d 560 (1979). Those convictions are therefore sustained.

(7) The evidence was sufficient to support **Warshak's** convictions for mail fraud, in violation of 18 U.S.C. § 1341. Those convictions are therefore sustained.

(8) The evidence was sufficient to support **Warshak's** and Harriet's respective convictions for bank fraud, in violation of 18 U.S.C. § 1344. Furthermore, the district court did not err in instructing the jury that, under certain circumstances, the government may prove specific intent to defraud a bank by showing specific intent to defraud a third party. *See United States v. Reaume,* 338 F.3d 577 (6th Cir.2003). Those convictions are therefore sustained.

(9) The evidence was sufficient to support **Warshak's** conviction for conspiracy to commit access-device fraud, in violation of 18 U.S.C. § 1029. That conviction is sustained.

(10) The evidence was sufficient to support **Warshak's** and TCI's respective convictions for money laundering, in violation of 18 U.S.C. §§ 1956, 1957. Those convictions are affirmed. By contrast, the evidence was insufficient to support Harriet's money-laundering convictions. Those convictions are therefore reversed.

(11) The evidence was sufficient to support **Warshak's** conviction for conspiracy to obstruct an FTC proceeding, in violation of 18 U.S.C. §§ 371, 1505. As a consequence, that conviction is sustained.

(12) The district court did not err in refusing to order the government to reveal whether or not it had conducted any additional surreptitious searches of **Warshak's** emails or communications. The discovery afforded by Federal Rule of Criminal Procedure 16 is limited to the evidence referred to in its express provisions, *United States v. Presser,* 844 F.2d 1275, 1285 (6th Cir.1988), and those provisions do not encompass the information sought by the defendants.

(13) The district court failed to provide an adequate explanation of its determination that the defendants should be held accountable for $411 million in losses. *See* Fed.R.Crim.P. 32(i)(3)(B); *United States v. White,* 492 F.3d 380, 415 (6th Cir.2007). We therefore vacate **Warshak's** sentence and remand.

(14) The district court did not abuse its discretion in refusing to admit certain evidence during the forfeiture phase of the trial. Furthermore, the evidence was sufficient to support the proceeds-money and money-laundering forfeiture judgments against **Warshak**. In addition, the evidence was sufficient to support the proceeds-money forfeiture judgment against Harriet, but it was insufficient to support the money-laundering forfeiture judgment against her. Therefore, the proceeds-money forfeiture judgment is affirmed with respect to both **Warshak** and Harriet, and the money-laundering money judgment is affirmed with respect to **Warshak**, but reversed with respect to Harriet.

*276 I. STATEMENT OF THE FACTS

A. Factual Background

In 2001, Steven **Warshak** ("**Warshak**") owned and operated a number of small businesses in the Cincinnati area. One of his businesses was TCI Media, Inc. ("TCI"), which sold advertisements in sporting venues. **Warshak** also owned a handful of companies that offered a modest line of so-called "nutraceuticals," or herbal supplements.[FN1] While the companies bore different names and sold different products, they appear to have been run as a single business, and they were later aggregated to form Berkeley Premium Nutraceuticals, Inc. ("Berkeley").[FN2] In Berkeley's early days, the company's workforce was relatively minute; the company employed approximately 12 to 15 people, nearly all of whom were **Warshak's** friends and family. Among them was his mother, Harriet **Warshak** ("Harriet"), who processed credit-card payments.

> FN1. The companies also sold a product called Keflex, which supposedly masked traces of drugs in one's urine.
>
> FN2. These companies were called Lifekey, Inc. (formed May 9, 2001); Boland Naturals, Inc. (formed May 7, 2002); Warner Health Care, Inc. (formed August 19, 2002); and

Wagner Nutraceuticals, Inc. (formed July 9, 2004). For the sake of simplicity, these entities will typically be referred to as Berkeley, even in cases where Berkeley was not yet in existence.

As the company grew, **Warshak** brought on additional employees to facilitate expansion, but he remained extremely "hands-on" with respect to the company's operations. In 2001, he hired James Teegarden, who eventually became Berkeley's Chief Operating Officer. **Warshak** also hired Shelley Kinmon to oversee the company's sales, later elevating her to the role of Vice-President. In 2002, Sue and Greg Cossman, **Warshak's** sister and brother-in-law, joined the company. Sue worked in Customer Care, where she dealt with customer complaints. Greg came in as the President of the company and thereafter functioned in various other capacities. That year also saw the hiring of Sam Grote, who was brought on board to work in the marketing department.

To sell its products, Berkeley took orders over the phone, but it also made sales through the mail and over the Internet. Customers purchased products with their credit cards, and their credit-card numbers were entered into a database along with other information. During sales calls, representatives would read from sales scripts,[FN3] which listed the major points to cover during the transaction. Shelley Kinmon testified that **Warshak** had the final word on the content of the scripts. Often, the scripts would include a description of the desired product, as well as language intended to persuade more pliant customers to make additional purchases.

FN3. Sales scripts were not employed at first.

In the latter half of 2001, Berkeley launched Enzyte, its flagship product. At the time of its launch, Enzyte was purported to increase the size of a man's erection. The product proved tremendously popular, and business rose sharply. By 2004, demand for Berkeley's products had grown so dramatically that the company employed 1500 people, and the call center remained open throughout the night, taking orders at breakneck speed. Berkeley's line of supplements also expanded, ballooning from approximately four products to around thirteen. By year's end, Berkeley's annual sales topped out at around $250 million, largely on the strength of Enzyte.

*277 1. *Advertising*

The popularity of Enzyte appears to have been due in large part to Berkeley's aggressive advertising campaigns. The vast majority of the advertising-approximately 98%-was conducted through television spots. Around 2004, network television was saturated with Enzyte advertisements featuring a character called "Smilin' Bob," whose trademark exaggerated smile was presumably the result of Enzyte's efficacy. The "Smilin' Bob" commercials were rife with innuendo and implied that users of Enzyte would become the envy of the neighborhood.

In addition to the television commercials, however, there were also advertisements in other media, such as print and radio. In 2001, just after Enzyte's premiere, advertisements appeared in a number of men's interest magazines. At **Warshak's** direction, those advertisements cited a 2001 independent customer study, which purported to show that, over a three-month period, 100 English-speaking men who took Enzyte experienced a 12 to 31% increase in the size of their penises. The 2001 study was also referenced in radio advertisements and appeared on the company's website, as well as in brochures and sales calls. James Teegarden later testified that the survey was bogus. He stated that, prior to the appearance of the advertisements, **Warshak** instructed him to create a spreadsheet and to fill it with fabricated data. Teegarden testified that he plucked the numbers out of the air and generated the spreadsheet over a twenty-four hour period.

A number of advertisements also indicated that Enzyte boasted a 96% customer satisfaction rating. Teegarden testified that that statistic, too, was totally spurious. Before the claim began showing up in Berkeley's literature, **Warshak** had asked him to harvest 500 names from the customer database and to "mark an 'X' by either satisfied or very satisfied on say 475 of those." As for the remaining 25, Teegarden "was to put not satisfied." Thereafter, the customer-satisfaction statistic cropped up in Berkeley's print advertisements and in the "sales pitches, brochures, [and on the] Internet."

Finally, numerous print and radio advertisements boasted that Enzyte was the brainchild of reputable doctors with impressive educational pedigrees. According to the ads, "Enzyte was developed by Dr.

Fredrick Thomkins, a physician with a biology degree from Stanford and Dr. Michael Moore, a leading urologist from Harvard." The ads also stated that the doctors had collaborated for thirteen years in developing a supplement designed to "stretch and elongate." In reality, the doctors were just as fictitious as "Smilin' Bob." Investigators who contacted Stanford and Harvard learned that neither man existed.

2. *The Auto-Ship Program*

The "life blood" of the business was its auto-ship program, which was instituted in 2001, shortly before Enzyte hit the market.[FN4] The auto-ship program was a continuity or negative-option program, in which a customer would order a free trial of a product and then continue to receive additional shipments of that product until he opted out. Before each new continuity shipment arrived on the customer's doorstep, a corresponding charge would appear on his credit-card statement. The shipments and charges would continue until the customer decided to withdraw from the ***278** program, which required the customer to notify the company.

FN4. In an email, **Warshak** noted, "[W]e break even on everything else. [Auto-ship] is our profit.-[I] cannot stress just how important it is that we get it right."

In the early days of the auto-ship program, customers who ordered products over the phone were not told that they were being enrolled.[FN5] From August 2001 to at least the end of December 2002,[FN6] customers were simply added to the program at the time of the initial sale without any indication that they would be on the hook for additional charges. Apparently, products were shipped with literature explaining the program, but no authorization was sought in advance of the shipment. According to Teegarden, **Warshak** explained that the auto-ship program was never mentioned because "nobody would sign up." If nobody signed up, "you couldn't make revenue."

FN5. Indeed, early sales scripts are entirely devoid of language indicating the existence of the auto-ship program.

FN6. Shelley Kinmon testified that, with respect to Enzyte, there was no disclosure of the auto-ship program in the sales scripts until September 23, 2003.

This policy resulted in a substantial volume of complaints, both to Berkeley and to outside organizations. In October 2002, the Better Business Bureau ("BBB") contacted Berkeley and indicated that more than 1,500 customers had called to voice their consternation. Because of the complaints, Berkeley's sales scripts and website began to include some language disclosing the auto-ship program.[FN7] A number of internal emails indicate that sales representatives were required to read the disclosure language and faced punishment if they failed to do so. To monitor the interactions between representatives and customers, Berkeley installed a recording system for all incoming calls.

FN7. The defendants also state that Berkeley hired "Venable [LLP], the most respected law firm in the area of direct marketing, in April 2003, to review its scripts and reformulate its disclosures[.]" Reply Br. at 6.

However, as a number of Berkeley insiders testified, the compulsory disclosure language was not always read, and it was designed not to work. Shelley Kinmon testified that the disclosure of the continuity shipments was only made *after* the customer had placed his order. In other words, the sales representative had already taken the customer's credit-card information when auto-ship was mentioned. Also, the disclosures were deliberately made with haste, and they were placed after unrelated language that was intended to divert or deaden the customer's attention. In the case of Enzyte, sales reps were instructed to lead into the disclosure language by stating that "the product is not a contraceptive nor will it prevent or treat any sexually transmitted disease." [FN8] According to Teegarden, the thinking was that, "if we started off with a statement about a contraceptive, something other than what it was, that people wouldn't really listen to what we were disclosing to them."

FN8. The disclosure portion of the September 23, 2003 sales script read, in full, as follows:

AFTER order is taken:

This product is not a contraceptive nor will it prevent any sexual disease. To let you know that with your order you would be

> part of our established customer program [*i.e.,* auto-ship] approx. 10 days before your current supply runs out you would receive a 2 month supply for the price of $69.95 with free shipping and handling. There is no obligation to remain on this program it is simple to discontinue, though it is a really good deal. All the reorder info is written on the side of your bottle when you receive your package, along with our phone number. So we will go ahead and process this order and have it to you within the next 5-7 business days. Thank you, *(customers [sic] name),* for your order today.

***279** Moreover, disclosure of the auto-ship program was sometimes irrelevant. For example, in November 2003, Berkeley hired a company called West to handle "sales calls that were from ... Avlimil or Enzyte advertisements." During the calls, West's representatives asked customers if they wanted to be enrolled in the auto-ship program, and over 80% of customers declined. When **Warshak** learned what was happening, he issued instructions to "take those customers, even if they decline[d], even if they said no to the Auto-Ship program, go ahead and put them on the Auto-Ship program." A subsequent email between Berkeley employees indicated that "all [West] customers, whether they know it or not, are going on [auto-ship]." As a result, numerous telephone orders resulted in unauthorized continuity shipments.

However, not all of Berkeley's auto-ship issues related to the telephone. Many Berkeley sales were the result of orders placed on the Internet, where disclosure of the auto-ship program was inconsistent. In 2001, when Berkeley was in its infancy, the company's websites contained no indication that customers would be enrolled in the program. Thereafter, disclosures were placed on the websites, but the disclosures would "appear[ ], disappear[ ], and chang[e]." In 2003, for instance, disclosure language that had been added to Berkeley's Avlimil website was removed because sales had been "drastically affected." Additionally, the language that did appear was often confusing and contained non sequiturs.

By July 2004, the complaints arising from Berkeley's auto-ship program had not slowed, so the President of the BBB reached out to Berkeley, sending a letter directly to **Warshak**. The purpose of the letter was to express "serious concerns about the number of complaints that [the BBB] had received." The complaints "related to a single issue, which was the [auto-ship] program." According to the President of the BBB, the organization "had asked on numerous occasions that [Berkeley] consider dropping [the program], and got no positive response."

3. *The Merchant Banks*

In order for Berkeley's business to operate, it was essential that the company be able to accept credit cards as a form of payment.[FN9] To process credit-card transactions, Berkeley obtained lines of credit from several merchant banks. The relationships between Berkeley and the merchant banks involved intermediaries known as credit-card processors. Often, the processors had contractual agreements with the merchant banks, and the processors were the ones who set up the credit-card processing arrangements with Berkeley. Nonetheless, when Berkeley applied for a merchant account with a given processor, the applications were passed along to the banks. Furthermore, either the banks or the processors could terminate Berkeley's merchant accounts.

> FN9. In the words of Greg Cossman, "without credit cards and the ability to charge them, there was no business."

In early 2002, **Warshak's** merchant account at the Bank of Kentucky was terminated for excessive "chargebacks." A chargeback occurs when a customer calls the credit card company directly and contests or disputes a charge. Merchant banks-and credit-card processors-will generally not do business with merchants that experience high volumes of chargebacks, as those merchants present a greater financial risk. In determining whether ***280** a merchant is experiencing excessive chargebacks, the banks refer to a figure known as the chargeback ratio, which is simply the percentage of transactions in a given 30-day period that result in a chargeback. For example, if a company conducts 100 credit-card transactions and one chargeback results, the company will have a chargeback ratio of 1%. Typically, if a merchant experiences more than one chargeback per hundred transactions, its chargeback ratio is deemed too high, resulting in fines and, eventually, termination of its accounts, either by the merchant bank or the credit-card processor.

Following the termination of the merchant account at the Bank of Kentucky, the company applied for merchant accounts with a number of other banks. In some instances, the applications, which often bore Harriet's signature, falsely listed her as the CEO and 100% owner of the company. In other instances, **Warshak** would complete the applications in his own name but falsely claim that he had never had a merchant account terminated. These prevarications were included in the applications because the prior termination would likely diminish Berkeley's chances of securing the services of other processors.

Despite its history with the Bank of Kentucky, Berkeley was able to land (or retain) merchant accounts with several processors. However, due to the auto-ship program and an extremely onerous refund policy,[FN10] Berkeley was repeatedly at risk of crossing the critical 1% chargeback threshold.[FN11] At company meetings, the chargeback ratio was a frequent topic of discussion, as was the possibility that Berkeley's accounts would be terminated. To prevent that from happening, a number of strategies were devised to artificially inflate the number of sales transactions and thus the denominator of the chargeback ratio, reducing that crucial ratio. One strategy was called "double-dinging." That practice involved splitting a single transaction into two, thereby driving up the number of transactions and diminishing the chargeback ratio. A double-ding might entail carving a $59.95 charge into a $54.95 charge for the product itself and a $5.00 charge for shipping. **Warshak** directed that virtually all sales be double-dinged, and by 2003, triple-dinging was initiated.

> FN10. Apparently, Berkeley's policy with respect to refunds was to "make it as difficult as possible." At one point, Enzyte customers seeking a refund were told they needed to obtain a notarized document indicating that they had experienced "no size increase." The admittedly ingenious idea behind the policy was that nobody "would actually go and have anything notarized that said that they had a small penis." In 2002, "there was really no refund policy. It was: Sorry, you got it, you keep it, and we'll cancel you off of future shipments." The defendants contend that this policy changed over time, suggesting that everyone who was entitled to a refund got a refund. However, there was language on the Enzyte website as late as 2006 indicating that "there are no refunds for orders once shipped."
>
> FN11. As Teegarden explained, the auto-ship program created a "problem because individuals, when they didn't know that they were getting charged, those individuals would try to call back in. They would try to get a credit back on their credit cards. They either had a hard time getting through to us, or we would deny them credit. And then they would have to go to their credit card companies and request a chargeback. That, in turn, increased our chargeback rate."

Another way the company depressed the chargeback ratio was to make numerous charges to **Warshak's** personal credit cards. At **Warshak's** behest, Berkeley employees would ring up $1.00 charges on each of his credit cards until their limits were reached. Apparently, the thinking ***281** was that this torrent of additional transactions would dilute the number of chargebacks and keep the ratio under 1%. The same thinking led the company to charge and then refund the credit cards of randomly selected customers. The charges were made without authorization, and if anyone complained about the odd activity on his card, he was told that it was the result of a computer glitch. Through the use of these techniques and others, the company was able to stave off termination of its merchant-bank accounts.

B. Procedural History

In September 2006, a grand jury sitting in the Southern District of Ohio returned a 112-count indictment charging **Warshak**, Harriet, TCI, and several others with various crimes related to Berkeley's business. **Warshak** was charged with conspiracy to commit mail, wire, and bank fraud (Count 1); mail fraud (Counts 2-13); making false statements to banks (Counts 14, 16-22, 24-26, 28); bank fraud (Counts 15, 23, 27); conspiracy to commit and attempt to commit access-device fraud (Count 29); conspiracy to commit money laundering (Count 34); money laundering (Counts 32-98, 102-106, 108); conspiracy to commit misbranding (Count 109); misbranding (Count 110); and, lastly, conspiracy to obstruct a Federal Trade Commission ("FTC") proceeding (Count 112). Harriet was charged with conspiracy to commit mail, wire,

and bank fraud (Count 1); bank fraud (Count 27); making false statements to a bank (Count 28); conspiracy to commit money laundering (Counts 30-31); and money laundering (Counts 99-101, 107). TCI was charged with money laundering (Counts 57-58, 60-73, 79, 83, 91-93).

Before trial, numerous motions were filed. First, **Warshak** moved to exclude thousands of emails that the government obtained from his Internet Service Providers. That motion was denied. **Warshak** also moved to bar the government from using any evidence "derived through improper access to privileged attorney-client communications." Appellant's Br. at 42. Following a " *Kastigar*-like" evidentiary hearing at which governmental inspectors testified that they did not make use of any privileged materials, the district court denied the motion. In addition, the defendants requested a continuance, which was denied.

Over fifteen months later, in January 2008, the case proceeded to trial. Approximately six weeks later, the trial ended and the defendants were convicted of the majority of the charges. **Warshak** was acquitted of Counts 14-22, 24-26, and 28, which charged him with making false statements to banks, and he was also acquitted of Counts 109-110, which charged him with misbranding offenses. Harriet was acquitted of Count 28, which alleged that she made false statements to a bank. She was convicted on Counts 27, 30-31, 99-101, and 107.

As soon as the trial was over, a forfeiture hearing was held, during which the jury heard additional evidence. At the hearing, the defendants attempted to introduce certain evidence that many of Berkeley's sales were legitimate, but the district court ruled that the evidence was irrelevant. When the hearing concluded, the jury found that the government had established the requisite nexus between certain assets and the crimes of both fraud and money laundering.

On August 27, 2008, the defendants were sentenced. **Warshak** received a sentence of 25 years of imprisonment. He was also ordered to pay a fine of $93,000 and a special assessment of $9,300. In addition, he was ordered to surrender $459,540,000 in proceeds-money-judgment forfeiture and $44,876,781.68 in money-laundering-***282** judgment forfeiture. Harriet was sentenced to 24 months of imprisonment, ordered to pay a special assessment of $800, and held jointly and severally liable for the forfeiture judgments. TCI was sentenced to five years of probation and ordered to pay a fine of $160,000 and a special assessment of $6,400.

Following a series of unsuccessful post-trial motions, the defendants timely appealed.

II. ANALYSIS

A. The Search & Seizure of Warshak's Emails

[1] **Warshak** argues that the government's warrantless, *ex parte* seizure of approximately 27,000 of his private emails constituted a violation of the Fourth Amendment's prohibition on unreasonable searches and seizures. [FN12] The government counters that, even if government agents violated the Fourth Amendment in obtaining the emails, they relied in good faith on the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701 et seq., a statute that allows the government to obtain certain electronic communications without procuring a warrant. The government also argues that any hypothetical Fourth Amendment violation was harmless. We find that the government *did* violate **Warshak's** Fourth Amendment rights by compelling his Internet Service Provider ("ISP") to turn over the contents of his emails. However, we agree that agents relied on the SCA in good faith, and therefore hold that reversal is unwarranted.[FN13]

FN12. This is not the first time **Warshak** has raised this argument. In ***Warshak v. United States***, 490 F.3d 455 (6th Cir.2007) (" ***Warshak I*** "), a panel of this court determined that **Warshak** did indeed have a privacy interest in the contents of his emails. That decision was vacated on ripeness grounds. *See* ***Warshak v. United States***, 532 F.3d 521 (6th Cir.2008) (en banc) (" ***Warshak II*** "). In the present case, **Warshak's** claim is ripe for review.

FN13. Though we may surely do so, we decline to limit our inquiry to the issue of good-faith reliance. *See Pearson v. Callahan*, 555 U.S. 223, 129 S.Ct. 808, 818, 172 L.Ed.2d 565 (2009). If every court confronted with a novel Fourth Amendment question were to skip directly to good faith, the government would be given *carte blanche* to violate constitutionally protected privacy rights, provided, of course, that a

> statute supposedly permits them to do so. The doctrine of good-faith reliance should not be a perpetual shield against the consequences of constitutional violations. In other words, if the exclusionary rule is to have any bite, courts must, from time to time, decide whether statutorily sanctioned conduct oversteps constitutional boundaries. *See id.* at 816 (noting that repeated avoidance of constitutional questions leads to "constitutional stagnation" (citing *Saucier v. Katz*, 533 U.S. 194, 201, 121 S.Ct. 2151, 150 L.Ed.2d 272 (2001))).

1. *The Stored Communications Act*

[2] The Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701 et seq., "permits a 'governmental entity' to compel a service provider to disclose the contents of [electronic] communications in certain circumstances." ***Warshak II***, 532 F.3d at 523. As this court explained in ***Warshak II***:

> Three relevant definitions bear on the meaning of the compelled-disclosure provisions of the Act. "[E]lectronic communication service[s]" permit "users ... to send or receive wire or electronic communications," [18 U.S.C.] § 2510(15), a definition that covers basic e-mail services, *see* Patricia L. Bellia et al., *Cyberlaw: Problems of Policy and Jurisprudence in the Information Age* 584 (2d ed. 2004). "[E]lectronic storage" is "any temporary, intermediate storage of a wire or electronic communication ... and ... any storage of such communication by an electronic communication service***283** for purposes of backup protection of such communication." 18 U.S.C. § 2510(17). "[R]emote computing service[s]" provide "computer storage or processing services" to customers, *id.* § 2711(2), and are designed for longer-term storage, *see* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L.Rev. 1208, 1216 (2004).
>
> The compelled-disclosure provisions give different levels of privacy protection based on whether the e-mail is held with an electronic communication service or a remote computing service and based on how long the e-mail has been in electronic storage. The government may obtain the contents of e-mails that are "in electronic storage" with an electronic communication service for 180 days or less "only pursuant to a warrant." 18 U.S.C. § 2703(a). The government has three options for obtaining communications stored with a remote computing service and communications that have been in electronic storage with an electronic service provider for more than 180 days: (1) obtain a warrant; (2) use an administrative subpoena; or (3) obtain a court order under § 2703(d). *Id.* § 2703(a), (b).

532 F.3d at 523-24 (some alterations in original).

2. *Factual Background*

Email was a critical form of communication among Berkeley personnel. As a consequence, **Warshak** had a number of email accounts with various ISPs, including an account with NuVox Communications. In October 2004, the government formally requested that NuVox prospectively preserve the contents of any emails to or from **Warshak's** email account. The request was made pursuant to 18 U.S.C. § 2703(f) and it instructed NuVox to preserve all future messages.[FN14] NuVox acceded to the government's request and began preserving copies of **Warshak's** incoming and outgoing emails-copies that would not have existed absent the prospective preservation request. Per the government's instructions, **Warshak** was not informed that his messages were being archived.

> FN14. **Warshak** appears to have accessed emails from his NuVox account via POP, or "Post Office Protocol." When POP is utilized, emails are downloaded to the user's personal computer and generally deleted from the ISP's server.

In January 2005, the government obtained a subpoena under § 2703(b) and compelled NuVox to turn over the emails that it had begun preserving the previous year. In May 2005, the government served NuVox with an *ex parte* court order under § 2703(d) that required NuVox to surrender any additional email messages in **Warshak's** account. In all, the government compelled NuVox to reveal the contents of approximately 27,000 emails. **Warshak** did not receive notice of either the subpoena or the order until May 2006.

3. *The Fourth Amendment*

[3] The Fourth Amendment provides that "[t]he right of the people to be secure in their persons,

houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause...." U.S. CONST. amend. IV. The fundamental purpose of the Fourth Amendment "is to safeguard the privacy and security of individuals against arbitrary invasions by government officials." *Camara v. Mun. Ct.*, 387 U.S. 523, 528, 87 S.Ct. 1727, 18 L.Ed.2d 930 (1967); *see Skinner v. Ry. Labor Execs.' Ass'n*, 489 U.S. 602, 613-14, 109 S.Ct. 1402, 103 L.Ed.2d 639 (1989) ("The [Fourth] Amendment***284** guarantees the privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the Government or those acting at their direction.").

[4] Not all government actions are invasive enough to implicate the Fourth Amendment. "The Fourth Amendment's protections hinge on the occurrence of a 'search,' a legal term of art whose history is riddled with complexity." *Widgren v. Maple Grove Twp.*, 429 F.3d 575, 578 (6th Cir.2005). A "search" occurs when the government infringes upon "an expectation of privacy that society is prepared to consider reasonable." *United States v. Jacobsen*, 466 U.S. 109, 113, 104 S.Ct. 1652, 80 L.Ed.2d 85 (1984). This standard breaks down into two discrete inquiries: "first, has the [target of the investigation] manifested a subjective expectation of privacy in the object of the challenged search? Second, is society willing to recognize that expectation as reasonable?" *California v. Ciraolo*, 476 U.S. 207, 211, 106 S.Ct. 1809, 90 L.Ed.2d 210 (1986) (citing *Smith v. Maryland*, 442 U.S. 735, 740, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979)).

Turning first to the subjective component of the test, we find that **Warshak** plainly manifested an expectation that his emails would be shielded from outside scrutiny. As he notes in his brief, his "entire business and personal life was contained within the ... emails seized." Appellant's Br. at 39-40. Given the often sensitive and sometimes damning substance of his emails,[FN15] we think it highly unlikely that **Warshak** expected them to be made public, for people seldom unfurl their dirty laundry in plain view. *See, e.g., United States v. Maxwell*, 45 M.J. 406, 417 (C.A.A.F.1996) ("[T]he tenor and content of e-mail conversations between appellant and his correspondent, 'Launchboy,' reveal a[n] ... expectation that the conversations were private."). Therefore, we conclude that **Warshak** had a subjective expectation of privacy in the contents of his emails.

FN15. In a number of the NuVox emails, **Warshak** discussed the creation of trusts for his children, as well as the possibility that his financial dealings would mislead FTC investigators.

The next question is whether society is prepared to recognize that expectation as reasonable. *See Smith*, 442 U.S. at 740, 99 S.Ct. 2577. This question is one of grave import and enduring consequence, given the prominent role that email has assumed in modern communication. *Cf. Katz*, 389 U.S. at 352, 88 S.Ct. 507 (suggesting that the Constitution must be read to account for "the vital role that the public telephone has come to play in private communication"). Since the advent of email, the telephone call and the letter have waned in importance, and an explosion of Internet-based communication has taken place. People are now able to send sensitive and intimate information, instantaneously, to friends, family, and colleagues half a world away. Lovers exchange sweet nothings, and businessmen swap ambitious plans, all with the click of a mouse button. Commerce has also taken hold in email. Online purchases are often documented in email accounts, and email is frequently used to remind patients and clients of imminent appointments. In short, "account" is an apt word for the conglomeration of stored messages that comprises an email account, as it provides an account of its owner's life. By obtaining access to someone's email, government agents gain the ability to peer deeply into his activities. Much hinges, therefore, on whether the government is permitted to request that a commercial ISP turn over the contents of a subscriber's emails without triggering the machinery of the Fourth Amendment.

***285** In confronting this question, we take note of two bedrock principles. First, the very fact that information is being passed through a communications network is a paramount Fourth Amendment consideration. *See ibid.*; *United States v. U.S. Dist. Court*, 407 U.S. 297, 313, 92 S.Ct. 2125, 32 L.Ed.2d 752 (1972) ("[T]he broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards."). Second, the Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish. *See Kyllo v. United States*, 533 U.S. 27, 34, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001)

(noting that evolving technology must not be permitted to "erode the privacy guaranteed by the Fourth Amendment"); *see also* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 Stan. L.Rev. 1005, 1007 (2010) (arguing that "the differences between the facts of physical space and the facts of the Internet require courts to identify new Fourth Amendment distinctions to maintain the function of Fourth Amendment rules in an online environment").

With those principles in mind, we begin our analysis by considering the manner in which the Fourth Amendment protects traditional forms of communication. In *Katz*, the Supreme Court was asked to determine how the Fourth Amendment applied in the context of the telephone. There, government agents had affixed an electronic listening device to the exterior of a public phone booth, and had used the device to intercept and record several phone conversations. *See* 389 U.S. at 348, 88 S.Ct. 507. The Supreme Court held that this constituted a search under the Fourth Amendment, *see id.* at 353, 88 S.Ct. 507, notwithstanding the fact that the telephone company had the capacity to monitor and record the calls, *see Smith*, 442 U.S. at 746-47, 99 S.Ct. 2577 (Stewart, J., dissenting). In the eyes of the Court, the caller was "surely entitled to assume that the words he utter[ed] into the mouthpiece w[ould] not be broadcast to the world." *Katz*, 389 U.S. at 352, 88 S.Ct. 507. The Court's holding in *Katz* has since come to stand for the broad proposition that, in many contexts, the government infringes a reasonable expectation of privacy when it surreptitiously intercepts a telephone call through electronic means. *Smith*, 442 U.S. at 746, 99 S.Ct. 2577 (Stewart, J., dissenting) ("[S]ince *Katz*, it has been abundantly clear that telephone conversations are fully protected by the Fourth and Fourteenth Amendments.").

Letters receive similar protection. *See Jacobsen*, 466 U.S. at 114, 104 S.Ct. 1652 ("Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy [.]"); *Ex Parte Jackson*, 96 U.S. 727, 733, 24 L.Ed. 877 (1877). While a letter is in the mail, the police may not intercept it and examine its contents unless they first obtain a warrant based on probable cause. *Ibid.* This is true despite the fact that sealed letters are handed over to perhaps dozens of mail carriers, any one of whom could tear open the thin paper envelopes that separate the private words from the world outside. Put another way, trusting a letter to an intermediary does not necessarily defeat a reasonable expectation that the letter will remain private. *See Katz*, 389 U.S. at 351, 88 S.Ct. 507 ("[W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.").

Given the fundamental similarities between email and traditional forms of communication, it would defy common sense ***286** to afford emails lesser Fourth Amendment protection. *See* Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-Mail*, 2008 U. Chi. Legal F. 121, 135 (2008) (recognizing the need to "eliminate the strangely disparate treatment of mailed and telephonic communications on the one hand and electronic communications on the other"); *City of Ontario v. Quon*, ---U.S. ----, 130 S.Ct. 2619, 2631, 177 L.Ed.2d 216 (2010) (implying that "a search of [an individual's] personal e-mail account" would be just as intrusive as "a wiretap on his home phone line"); *United States v. Forrester*, 512 F.3d 500, 511 (9th Cir.2008) (holding that "[t]he privacy interests in [mail and email] are identical"). Email is the technological scion of tangible mail, and it plays an indispensable part in the Information Age. Over the last decade, email has become "so pervasive that some persons may consider [it] to be [an] essential means or necessary instrument[ ] for self-expression, even self-identification." *Quon*, 130 S.Ct. at 2630. It follows that email requires strong protection under the Fourth Amendment; otherwise, the Fourth Amendment would prove an ineffective guardian of private communication, an essential purpose it has long been recognized to serve. *See U.S. Dist. Court*, 407 U.S. at 313, 92 S.Ct. 2125; *United States v. Waller*, 581 F.2d 585, 587 (6th Cir.1978) (noting the Fourth Amendment's role in protecting "private communications"). As some forms of communication begin to diminish, the Fourth Amendment must recognize and protect nascent ones that arise. *See* ***Warshak I***, 490 F.3d at 473 ("It goes without saying that like the telephone earlier in our history, e-mail is an ever-increasing mode of private communication, and protecting shared communications through this medium is as important to Fourth Amendment principles today as protecting telephone conversations has been in the past.").

If we accept that an email is analogous to a letter

or a phone call, it is manifest that agents of the government cannot compel a commercial ISP to turn over the contents of an email without triggering the Fourth Amendment. An ISP is the intermediary that makes email communication possible. Emails must pass through an ISP's servers to reach their intended recipient. Thus, the ISP is the functional equivalent of a post office or a telephone company. As we have discussed above, the police may not storm the post office and intercept a letter, and they are likewise forbidden from using the phone system to make a clandestine recording of a telephone call-unless they get a warrant, that is. *See* Jacobsen, 466 U.S. at 114, 104 S.Ct. 1652; Katz, 389 U.S. at 353, 88 S.Ct. 507. It only stands to reason that, if government agents compel an ISP to surrender the contents of a subscriber's emails, those agents have thereby conducted a Fourth Amendment search, which necessitates compliance with the warrant requirement absent some exception.

In ***Warshak I***, the government argued that this conclusion was improper, pointing to the fact that NuVox contractually reserved the right to access **Warshak's** emails for certain purposes. While we acknowledge that a subscriber agreement might, in some cases, be sweeping enough to defeat a reasonable expectation of privacy in the contents of an email account, *see* ***Warshak I***, 490 F.3d at 473; ***Warshak II***, 532 F.3d at 526-27, we doubt that will be the case in most situations, and it is certainly not the case here.

As an initial matter, it must be observed that the mere *ability* of a third-party intermediary to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy.***287** In Katz, the Supreme Court found it reasonable to expect privacy during a telephone call despite the ability of an operator to listen in. *See* Smith, 442 U.S. at 746-47, 99 S.Ct. 2577 (Stewart, J., dissenting). Similarly, the ability of a rogue mail handler to rip open a letter does not make it unreasonable to assume that sealed mail will remain private on its journey across the country. Therefore, the threat or possibility of access is not decisive when it comes to the reasonableness of an expectation of privacy.

Nor is the *right* of access. As the Electronic Frontier Foundation points out in its *amicus* brief, at the time Katz was decided, telephone companies had a right to monitor calls in certain situations. Specifically, telephone companies could listen in when reasonably necessary to "protect themselves and their properties against the improper and illegal use of their facilities." Bubis v. United States, 384 F.2d 643, 648 (9th Cir.1967). In this case, the NuVox subscriber agreement tracks that language, indicating that "NuVox *may* access and use individual Subscriber information in the operation of the Service and as necessary to protect the Service." Acceptable Use Policy, *available at* http:// business. windstream. com/ Legal/ acceptable Use. htm (last visited Aug. 12, 2010). Thus, under Katz, the degree of access granted to NuVox does not diminish the reasonableness of **Warshak's** trust in the privacy of his emails.[FN16]

> FN16. We note that the access granted to NuVox was also temporally limited, as **Warshak's** email account was configured to delete his emails from NuVox's servers as soon as he opened them on his personal computer. *See* Appellant's Br. at 28 ("NuVox did not even save copies of account holders' received emails once they had been opened and downloaded to the account holders' computers[.]").

Our conclusion finds additional support in the application of Fourth Amendment doctrine to rented space. Hotel guests, for example, have a reasonable expectation of privacy in their rooms. *See* United States v. Allen, 106 F.3d 695, 699 (6th Cir.1997). This is so even though maids routinely enter hotel rooms to replace the towels and tidy the furniture. Similarly, tenants have a legitimate expectation of privacy in their apartments. *See* United States v. Washington, 573 F.3d 279, 284 (6th Cir.2009). That expectation persists, regardless of the incursions of handymen to fix leaky faucets. Consequently, we are convinced that some degree of routine access is hardly dispositive with respect to the privacy question.

Again, however, we are unwilling to hold that a subscriber agreement will *never* be broad enough to snuff out a reasonable expectation of privacy. As the panel noted in ***Warshak I***, if the ISP expresses an intention to "audit, inspect, and monitor" its subscriber's emails, that might be enough to render an expectation of privacy unreasonable. *See* 490 F.3d at 472-73 (quoting United States v. Simons, 206 F.3d 392, 398 (4th Cir.2000)). But where, as here, there is no such statement, the ISP's "control over the [emails] and ability to access them under certain limited cir-

cumstances will not be enough to overcome an expectation of privacy." *Id.* at 473.

We recognize that our conclusion may be attacked in light of the Supreme Court's decision in *United States v. Miller*, 425 U.S. 435, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976). In *Miller*, the Supreme Court held that a bank depositor does not have a reasonable expectation of privacy in the contents of bank records, checks, and deposit slips. *Id.* at 442, 96 S.Ct. 1619. The Court's holding in *Miller* was based on the fact that bank documents, "including financial statements and deposit slips, contain ***288** only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business." *Ibid.* The Court noted,

> The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government.... [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.

Id. at 443, 96 S.Ct. 1619 (citations omitted).

But *Miller* is distinguishable. First, *Miller* involved simple business records, as opposed to the potentially unlimited variety of "confidential communications" at issue here. *See ibid.* Second, the bank depositor in *Miller* conveyed information to the bank so that the bank could put the information to use "in the ordinary course of business." *Ibid.* By contrast, **Warshak** received his emails through NuVox. NuVox was an *intermediary,* not the intended recipient of the emails. *See* Bellia & Freiwald, *Stored E-Mail*, 2008 U. Chi. Legal F. at 165 ("[W]e view the best analogy for this scenario as the cases in which a third party carries, transports, or stores property for another. In these cases, as in the stored e-mail case, the customer grants access to the ISP because it is essential to the customer's interests."). Thus, *Miller* is not controlling.

[5] Accordingly, we hold that a subscriber enjoys a reasonable expectation of privacy in the contents of emails "that are stored with, or sent or received through, a commercial ISP." ***Warshak I***, 490 F.3d at 473; *see Forrester*, 512 F.3d at 511 (suggesting that "[t]he contents [of email messages] may deserve Fourth Amendment protection"). The government may not compel a commercial ISP to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable cause. Therefore, because they did not obtain a warrant, the government agents violated the Fourth Amendment when they obtained the contents of **Warshak's** emails. Moreover, to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional.

4. *Good-Faith Reliance*

[6] Even though the government's search of **Warshak's** emails violated the Fourth Amendment, the emails are not subject to the exclusionary remedy if the officers relied in good faith on the SCA to obtain them. *See Krull*, 480 U.S. at 349-50, 107 S.Ct. 1160. In *Krull*, the Supreme Court noted that the exclusionary rule's purpose of deterring law enforcement officers from engaging in unconstitutional conduct would not be furthered by holding officers accountable for mistakes of the legislature. *Ibid.* Thus, even if a statute is later found to be unconstitutional, an officer "cannot be expected to question the judgment of the legislature." *Ibid.* However, an officer cannot "be said to have acted in good-faith reliance upon a statute if its provisions are such that a reasonable officer should have known that the statute was unconstitutional." *Id.* at 355, 107 S.Ct. 1160.

Naturally, **Warshak** argues that the provisions of the SCA at issue in this case were plainly unconstitutional. He argues that any reasonable law enforcement officer would have understood that a warrant based on probable cause would be required to compel the production of private emails. In making this argument, he leans heavily on ***Warshak I***, which opined that the SCA permits agents to engage in searches "that ***289** clearly do not comport with the Fourth Amendment." 490 F.3d at 477.

However, we disagree that the SCA is so conspicuously unconstitutional as to preclude good-faith reliance. As we noted in ***Warshak II***, "[t]he Stored Communications Act has been in existence since 1986 and to our knowledge has not been the subject of any successful Fourth Amendment challenges, in any context, whether to § 2703(d) or to any other provision." 532 F.3d at 531. Furthermore, given the complicated thicket of issues that we were required to

navigate when passing on the constitutionality of the SCA, it was not plain or obvious that the SCA was unconstitutional, and it was therefore reasonable for the government to rely upon the SCA in seeking to obtain the contents of **Warshak's** emails.[FN17]

> FN17. Of course, after today's decision, the good-faith calculus has changed, and a reasonable officer may no longer assume that the Constitution permits warrantless searches of private emails.

But the good-faith reliance inquiry does not end with the facial validity of the statute at issue. In *Krull*, the Supreme Court hinted that the good-faith exception does not apply if the government acted "outside the scope of the statute" on which it purported to rely. 480 U.S. at 360 n. 17, 107 S.Ct. 1160. It should be noted that this portion of the *Krull* Court's opinion was merely dicta, and it appears that we have yet to pass on the question. However, it seems evident that an officer's failure to adhere to the boundaries of a given statute should preclude him from relying upon it in the face of a constitutional challenge.[FN18] Once the officer steps outside the scope of an unconstitutional statute, the mistake is no longer the legislature's, but the officer's. *See ibid.* ("In that context, the relevant actors are not legislators or magistrates, but police officers who concededly are engaged in the often competitive enterprise of ferreting out crime." (citation and internal quotation marks omitted)). Therefore, use of the exclusionary rule is once again efficacious in deterring officers from engaging in conduct that violates the Constitution. *Ibid.*

> FN18. At least one court has translated this inquiry into the context of qualified immunity. In *Roska ex rel. Roska v. Sneddon*, 437 F.3d 964 (10th Cir.2006), the Tenth Circuit considered whether an officer's alleged reliance on a state statute rendered his conduct objectively reasonable. The court held that, in determining whether such reliance had occurred, one fact to consider was "whether the official in fact complied with the statute." *Id.* at 971.

Warshak argues that the government violated several provisions of the SCA and should therefore be precluded from arguing good-faith reliance. First, **Warshak** argues that the government violated the SCA's notice provisions. Under § 2703(b)(1)(B), the government must provide notice to an account holder if it seeks to compel the disclosure of his emails through either a § 2703(b) subpoena or a § 2703(d) order. However, § 2705 permits the government to delay notification in certain situations. The initial period of delay is 90 days, but the government may seek to extend that period in 90-day increments. In this case, the government issued both a § 2703(b) subpoena and a § 2703(d) order to NuVox, seeking disclosure of **Warshak's** emails. At the time, the government made the requisite showing that notice should be delayed. However, the government did not seek to renew the period of delay. In all, the government failed to inform **Warshak** of either the subpoena or the order for over a year.

Conceding that it violated the notice provisions, the government argues that such violations are irrelevant to the issue of whether it reasonably relied on the ***290** SCA in *obtaining* the contents of **Warshak's** emails. We agree. As the government notes, the violations occurred *after* the emails had been obtained. Thus, the mistakes at issue had no bearing on the constitutional violations. Because the exclusionary rule was designed to deter constitutional violations, we decline to invoke it in this situation.

But **Warshak** does not hang his hat exclusively on the government's violations of the SCA's notice provisions. He also argues that the government exceeded its authority under another SCA provision- § 2703(f)-by requesting NuVox to engage in *prospective* preservation of his future emails.[FN19] Under § 2703(f), "[a] provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to *preserve* records and other evidence *in its possession* pending the issuance of a court order or other process." 18 U.S.C. § 2703(f) (emphasis added). **Warshak** argues that this statute permits only *retrospective* preservation-in other words, preservation of emails already in existence. He notes that the Department of Justice ("DOJ") generally agrees with his construction of the statute, pointing to the DOJ's own computer-surveillance manual, which states: "[Section] 2703(f) letters should not be used prospectively to order providers to preserve records not yet created. If agents want providers to record information about future electronic communications, they should comply with the [Wiretap Act and the Pen/Trap stat-

ute]." FN20

FN19. It appears that, below, **Warshak** argued that the preservation request was itself a violation of the Fourth Amendment. He does not renew that argument on appeal, and it is therefore waived. *See Robinson v. Jones*, 142 F.3d 905, 906 (6th Cir.1998) ("Issues which were raised in the district court, yet not raised on appeal, are considered abandoned and not reviewable on appeal.").

FN20. **Warshak** also argues that the government's § 2703(f) request for prospective preservation of his emails was a violation of the Wiretap Act. However, the government does not plead reliance on the Wiretap Act to justify its actions. Thus, this argument is immaterial.

Ultimately, however, this statutory violation, whether it occurred or not, FN21 is irrelevant to the issue of good-faith reliance. The question here is whether the government relied in good faith on § 2703(b) and § 2703(d) to *obtain* copies of **Warshak's** emails. True, the government might not have been able to gain access to the emails without the prospective preservation request, as it was NuVox's practice to delete all emails once they were downloaded to the account holder's computer. Thus, in a sense, the government's use of § 2703(f) was a but-for cause of the constitutional violation. But the actual violation at issue was obtaining the emails, and the government did not rely on § 2703(f) specifically to do that. Instead, the government relied on § 2703(b) and § 2703(d). The proper inquiry, therefore, is whether the government violated either of *those* provisions, and the preservation request is of no consequence to that inquiry.

FN21. Some courts and commentators have suggested that § 2703(f) applies only retroactively. *See, e.g.,* Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 Geo. Wash. L.Rev. 1557, 1565 (2004) ("The Wiretap Act and Pen Register statute regulate prospective surveillance of Internet communications (communications "in transit"), and the SCA governs retrospective surveillance (stored communications)."). However, the language of the statute, on its face, does not compel this reading.

Warshak's next argument is that the government violated § 2703(d) by failing to provide any particularized factual basis ***291** when seeking an order for disclosure. Under § 2703(d), such an order "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 ... are relevant and material to an ongoing criminal investigation."

To the extent that he is arguing that the government's application was insufficient, **Warshak** is wrong. The government's application indicated that it was "investigating a complex, large-scale mail and wire fraud operation based in Cincinnati, Ohio." The application also indicated that "interviews of current and former employees of the target company suggest that electronic mail is a vital communication tool that has been used to perpetuate the fraudulent conduct." Additionally, the application observed that "various sources [have verified] that NuVox provides electronic communications services to certain individual(s) [under] investigation." In light of these statements, it is clear that the application was, in fact, supported by specific and articulable facts, especially given the diminished standard that applies to § 2703(d) applications. *See United States v. Perrine*, 518 F.3d 1196, 1202 (10th Cir.2008) (noting that "the 'specific and articulable facts' standard derives from the Supreme Court's decision in *Terry* "); ***Warshak I***, 490 F.3d at 463 ("The parties agree that the standard of proof for a court order-'specific and articulable facts showing that there are reasonable grounds to believe that the contents ... or records ... are relevant and material to an ongoing criminal investigation'-falls short of probable cause.").

Finally, **Warshak** argues that a finding of good-faith reliance is improper because the government presented the magistrate with an erroneous definition of the term "electronic storage." As noted above, if an email is in electronic storage for less than 180 days, the government may not compel its disclosure without a warrant. 18 U.S.C. § 2703(a). In applying for the subpoena and the order that eventually resulted in the disclosure of **Warshak's** NuVox emails, the government suggested to the magistrate

that an email is not in electronic storage if it has already been "accessed, viewed, or downloaded." **Warshak** argues that this definition of electronic storage does not comport with the Ninth Circuit's decision in *Theofel v. Farey-Jones*, 359 F.3d 1066, 1071 (9th Cir.2004), which held that "prior access is irrelevant to whether the [emails] at issue were in electronic storage." **Warshak** further argues that, because the government failed to mention the Ninth Circuit's definition, it "usurped the court's function to determine whether an email ... [is] in 'electronic storage [.]' " Appellant's Br. at 38.

As an initial matter, it is manifest that the decisions of the Ninth Circuit are not binding on courts in this circuit. It therefore cannot be said that the government somehow violated § 2703 by failing to cite an out-of-circuit decision that it thought to be wrongly decided. Incidentally, the government is not alone in thinking that the Ninth Circuit's definition of electronic storage is incorrect. One commentator has noted that " *Theofel* is quite implausible and hard to square with the statutory test." Kerr, *A User's Guide to the Stored Communications Act*, 72 Geo. Wash. L.Rev. at 1217; *see also United States v. Weaver*, 636 F.Supp.2d 769, 773 (C.D.Ill.2009) ("Previously opened emails stored by Microsoft for Hotmail users are not in electronic storage, and the Government can obtain copies of such emails using a trial subpoena.").

Furthermore, it does a disservice to the magistrate judge to suggest that the government usurped the role of the court. ***292** The government's application did include a proposed definition of the term "electronic storage." That does not mean, however, that the magistrate judge unhesitatingly received that definition, and, as the government notes, the magistrate "presumably [had] the opportunity to consider and review relevant precedent." Appellee's Br. at 117.

Consequently, we find that, although the government violated the Fourth Amendment, the exclusionary rule does not apply, as the government relied in good faith on § 2703(b) and § 2703(d) to access the contents of **Warshak's** emails.[FN22]

> FN22. In addition, we note that the Fourth Amendment violation was likely harmless. *See United States v. Carnes*, 309 F.3d 950, 963 (6th Cir.2002) (noting that a Fourth Amendment violation does not warrant reversal if the violation was harmless). The NuVox emails did not play a role in obtaining the search warrant that produced the overwhelming majority of the evidence in this case. In addition, only three of the emails were introduced at trial, and they were largely cumulative of the testimony of William Bertemes, **Warshak's** accountant. *See Bradley v. Cowan*, 561 F.2d 1213, 1217 (6th Cir.1977) (noting that the impact of "purely cumulative" evidence is often minimal).

B. The *Kastigar*-Like Hearing

1. *Background*

During the government's investigation of Berkeley, case agents came into possession of myriad documents that were ostensibly subject to the attorney-client privilege. Many of the documents were obtained during a March 16, 2005 search of Berkeley's headquarters, in which agents copied the contents of over 90 computers. Other documents were procured earlier through the subpoena and court order issued to NuVox, which granted investigators access to the contents of **Warshak's** email accounts. In all, case agents had access to approximately "60,000 email communications from or to attorneys representing Berkeley and **Warshak**, communications facially and presumptively protected by the attorney-client privilege." Appellant's Br. at 41.

[7] On July 5, 2007, **Warshak** filed a "motion to bar the government from using the evidence obtained in violation of the defendants' attorney-client and work product privileges and to dismiss the indictment since privileged material was used to secure it." *United States v. **Warshak***, No. 1:06-CR-00111, 2007 WL 3306603, at *1 (S.D.Ohio Nov.5, 2007). In the motion, the defendants requested that the district court hold a hearing "in the framework of *Kastigar v. United States*, 406 U.S. 441, 92 S.Ct. 1653, 32 L.Ed.2d 212 (1972), at which the government would bear the burden of establishing that its case was untainted by attorney-client and work product privileged materials." ***Warshak***, 2007 WL 3306603, at *1. To an extent, the district court granted the motion, setting a " *Kastigar*-like" hearing with the "narrow purpose of eliciting the sworn testimony of government agents as to their handling of evidence." *Ibid.* In ordering the hearing, the district court "found that [the]

[d]efendants had raised enough of a question about the amount of time U.S. Postal Inspector Alejandro Almaguer ('Almaguer') possessed privileged data, as well as the government's methodology in screening data for privileged information, to merit a response." *Ibid.*

The hearing was held on September 27 and 28, 2007. During the hearing, "the government proffered evidence and the testimony of Almaguer, the [d]efendants were afforded [an] opportunity to cross-examine Almaguer and examine other agents on direct, and the parties argued their respective positions concerning the ***293** propriety of the government action in this case." *Ibid.* In addition, the defendants called Peter Horstmann, an expert witness "who used software to analyze the electronic documents the government produced to [the] [d]efendants." *Ibid.*

After the hearing, the district court held that the government had satisfied its burden, stating as follows:

> The [c]ourt's original concerns that triggered the grant of the " *Kastigar*-like" evidentiary hearing were rooted in the amount of time that Almaguer allegedly had access to privileged materials, and in the fact the government had proffered no sworn statements backing its contention that it did not use privileged materials to obtain witness proffers. The government has completely allayed the [c]ourt's concerns. The United States has met its burden to demonstrate its agents have acted properly and that its case is untainted by privileged information.
>
> *Id.* at *8.

2. *The Adequacy of the Government's Presentation*

[8] **Warshak** argues that the *Kastigar*-like hearing was inadequate. More precisely, he argues that the district court failed to "hold[ ] the government to the burden prescribed by *Kastigar* and subsequent cases applying it." Appellant's Br. at 48. He complains that the district court "simply accepted the government's blanket denials that it used privileged materials in preparing its case against defendants, and shifted the burden to [him] to show that privileged materials contributed to the return of the indictment." *Ibid.* (internal citations omitted). In short, he argues that the district court improperly loosened the stringent demands of *Kastigar*.

In *Kastigar*, the Supreme Court held that when a witness is compelled to give incriminating testimony under a grant of statutory immunity and is thereafter prosecuted for any matter related to the compelled testimony, the government must shoulder the "heavy burden of proving that all of the evidence it proposes to use was derived from legitimate independent sources." 406 U.S. at 461-62, 92 S.Ct. 1653; *see also United States v. Turner*, 936 F.2d 221, 224 (6th Cir.1991). "This burden of proof ... is not limited to a negation of taint; rather, it imposes on the prosecution the affirmative duty to prove that the evidence it proposes to use is derived from a legitimate source wholly independent of the compelled testimony." *Kastigar*, 406 U.S. at 460, 92 S.Ct. 1653.

While *Kastigar* is clearly concerned with the use of testimony obtained despite an assertion of the Fifth Amendment privilege against self-incrimination, this court has suggested that *Kastigar* concerns may arise in the context of other privileges, such as the privilege accorded to attorney-client communications. Specifically, this court has hinted, in dicta, that "the leaking of privileged materials to investigators would raise the spectre of *Kastigar*-like evidentiary hearings." *In re Grand Jury Subpoenas*, 454 F.3d 511, 517 (6th Cir.2006). However, no other appellate court appears to have joined us in suggesting that *Kastigar* is implicated whenever investigators come into possession of materials subject to the attorney-client privilege.

One circuit, the Fourth, has engaged in a fairly lengthy analysis of *Kastigar* 's applicability in the arena of non-constitutional privileges. In *United States v. Squillacote*, 221 F.3d 542 (4th Cir.2000), the Fourth Circuit was faced with a scenario in which government investigators had legally conducted electronic surveillance on several defendants pursuant to the Foreign ***294** Intelligence Surveillance Act.[FN23] During the surveillance, the agents heard and recorded a number of conversations between one of the defendants and her psychotherapists. Subsequently, the defendants "moved to suppress any evidence derived from the privileged communications," arguing that "they were entitled to a hearing to vindicate the principles set forth by the Supreme Court in [*Kastigar*]." *Id.* at 558. Ultimately, the court determined that *Kastigar* was "simply ... not applicable." *Ibid.*

FN23. That is to say, the federal agents had

> established probable cause to believe that the targets of the surveillance were a foreign power or agents of a foreign power. *Squillacote,* 221 F.3d at 554; *see* 50 U.S.C. § 1804(a).

In so holding, the *Squillacote* court began by conceding that the conversations at issue, which the government had obtained during surveillance, were privileged. According to the court, "[t]he question, then, [was] whether the mere existence of this privileged information br[ought] to bear the full weight of *Kastigar.*" *Id.* at 559. The court held that it did not, finding that "a *Kastigar* analysis is not triggered by the existence of evidence protected by a privilege, but instead by the government's *effort to compel* a witness to testify over the witness's claim of privilege." *Ibid.* (emphasis added). However, the court also opined "that *Kastigar*-like protections may be required in cases involving testimony compelled over the assertion of a non-constitutional privilege." *Ibid.* Nonetheless, in concluding its analysis, the court reiterated that "because the government's right to compel testimony in the face of a claim of privilege is the issue at the heart of *Kastigar,* its protections do not apply in cases where there is privileged evidence, but no compelled testimony." *Id.* at 560. We agree, and hold that, absent compelled testimony, the full protections of *Kastigar* are inapplicable.

As further justification for its holding in *Squillacote,* the Fourth Circuit observed that "suppression of any evidence derived from the privileged conversations would be [im]proper in this case, given that the privilege is a testimonial or evidentiary one, and not constitutionally-based." *Ibid.* In making this assertion, the court observed that, as of the year 2000, no court had applied the fruit-of-the-poisonous-tree doctrine to derivative evidence obtained as a result of improper access to materials covered by a non-constitutional privilege. *Ibid.* (quoting *United States v. Marashi,* 913 F.2d 724, 731 n. 11 (9th Cir.1990)); *see also Nickel v. Hannigan,* 97 F.3d 403, 409 (10th Cir.1996) ("[W]e decline to apply the 'fruit of the poisonous tree' doctrine to the possible breach of attorney-client privilege in this case."). We have found no subsequent authority indicating that such derivative evidence is subject to suppression, and we agree that it is unwise to extend the fruit-of-the-poisonous-tree doctrine beyond the context of constitutional violations. *See Trammel v. United States,* 445 U.S. 40, 51, 100 S.Ct. 906, 63 L.Ed.2d 186 (1980) (indicating that testimonial privileges must be balanced against "the need for probative evidence in the administration of criminal justice").

In the present case, the privileged materials were not obtained from **Warshak** as a result of compelled testimony. Instead, they were garnered pursuant to a subpoena, a court order, and a search warrant, much like the psychotherapist-patient conversations at issue in *Squillacote.* Thus, because the documents were not the product of compelled testimony, a full *Kastigar* hearing was not required. Moreover, there is no indication that the government made any direct use of the privileged communications,***295** either at trial or before the grand jury. Consequently, given the fact that evidence derived from a violation of the attorney-client privilege is not fruit of the poisonous tree, **Warshak's** argument withers.

C. Volume & Format of Discovery

The volume of discovery in the present case was prodigious. Indeed, the government turned over millions of pages of discovery, but that discovery appears to have come from relatively few sources. Most of the discovery came from Berkeley itself, when, in March 2005, inspectors executed a search warrant and "imaged" (i.e., copied) the electronic contents of the company's computers and servers. After the search, the computers and servers remained on Berkeley's premises, except for several laptops, which were taken offsite and returned two days later. All told, the electronic evidence originating at Berkeley filled three "tera-drives" and numbered 17 million pages. In addition to the electronic evidence, agents seized approximately 506,000 pages of hard-copy documents, all of which the defendants were eventually permitted to copy. On top of the evidence obtained at Berkeley, discovery included 275 discs of material gathered by the grand jury and 13 discs of potential trial exhibits compiled by the government.

The defendants make three arguments with respect to the immense volume of discovery in this case. First, they argue that the district court abused its discretion and violated their right to a fair trial by allowing the government to turn over stupendous quantities of evidence in a disorganized and unsearchable format. Next, they argue that the government was improperly permitted to "abdicate" its *Brady* obliga-

tions by producing gargantuan "haystacks" of discovery that swallowed any "needles" of exculpatory information. Appellant's Br. at 52. Finally, the defendants argue that the district court erroneously denied a 90-day continuance, which was requested to enable the defendants to continue sifting through the mountains of discovery furnished by the government. Ultimately, none of these arguments is persuasive.[FN24]

> FN24. In making their discovery-related arguments, the defendants contend that the alleged errors should be evaluated collectively. That is, the defendants contend that the alleged mistakes combined to result in a violation of due process and the right to a fair trial. However, the aggregate impact of these supposed evils does not rise to the level of a constitutional violation.

1. *The Manner in Which the Government Produced Discovery*

The defendants' first argument is that the district court erroneously permitted the government to produce titanic amounts of electronic discovery in formats that were simultaneously disorganized and unsearchable. Specifically, the defendants assert that the electronic images of the Berkeley computers and the discs of potential trial exhibits were difficult to search. The defendants further contend that the government's failure to supplement the discovery materials with indices was prejudicial to the preparation of an adequate defense.[FN25] In making this argument, the defendants lean heavily on Federal Rule of *Civil* Procedure 34(b)(2)(E)(i), which requires a party to "produce [discovery materials] as they are kept in the usual course of business or [to] organize and label them to correspond to the categories in the request." The defendants acknowledge that there is no corresponding provision in ***296**Federal Rule of *Criminal* Procedure 16, which governs criminal discovery, but they argue that due process mandates enforcement of the civil rule in the criminal context.

> FN25. The defendants concede that "[t]he government provided indices to some of the hard-copy discovery." Appellant's Br. at 52 n. 16.

[9] A district court's decision on a discovery matter is reviewed for abuse of discretion. *United States v. Gray*, 521 F.3d 514, 529 (6th Cir.2008) (citing *United States v. $174,206.00 in U.S. Currency*, 320 F.3d 658, 663 (6th Cir.2003)); *see United States v. Maples*, 60 F.3d 244, 246 (6th Cir.1995) ("It is well settled that a district court has considerable discretion under Rule 16....").

[10] As an initial matter, it must be noted that the defendants cite scant authority suggesting that a district court must order the government to produce electronic discovery in a particular fashion.[FN26] Furthermore, it bears noting that Federal Rule of Criminal Procedure 16, which governs discovery in criminal cases, is entirely silent on the issue of the form that discovery must take; it contains no indication that documents must be organized or indexed. Thus, if we are to find that the district court abused its discretion, we must do so despite a pronounced dearth of precedent suggesting that the district court was wrong.

> FN26. In suggesting that criminal discovery must comply with Rule 34(b), the defendants point to a single case, namely, *United States v. O'Keefe*, 537 F.Supp.2d 14 (D.D.C.2008). There, the district court looked to Federal Rule of Civil Procedure 34(b) in assessing the form in which the government should produce documents. *Id.* at 19. However, the *O'Keefe* court admitted that, "[i]n criminal cases, there is unfortunately no rule to which the courts can look for guidance in determining whether the production of documents by the government has been in a form or format that is appropriate." *Id.* at 18-19.

[11] There are a number of factors that counsel against such a finding. First, the overwhelming majority of the discovery at issue was taken directly from Berkeley's computers, which means the defendants had ready access to that information. It also means that the defendants had access to the documents "as they [were] kept in the usual course of business." Fed.R.Civ.P. 34(b)(2)(E)(i). Thus, any difficulty that the defendants had in accessing the copies is arguably immaterial.[FN27]

> FN27. Moreover, any disorganization in the documents was likely attributable to the defendants themselves. It cannot be that the government is necessarily responsible for curing the disarray that they inherited.

Furthermore, there is reason to believe that the defendants were experiencing little difficulty in accessing the contents of the electronic discovery. Though the defendants claim that they were provided with data that had been rendered in unsearchable formats, they were citing discovery material to the district court in their motions, leading the district court to observe that the "[d]efendants' motion[s] demonstrate[d] [that] they [were] capably navigating discovery." Additionally, at the *Kastigar*-like hearing held before the district court, an expert witness who testified for the defense indicated that, with the use of certain software, he could perform "very quick and thorough" searches of the electronic discovery. Consequently, it does not appear that the discovery materials were nearly as unsearchable as the defense purports.

Lastly, it should be observed that the government did provide the defense with something of a guide to the electronic discovery. In response to the defense's discovery request, the government furnished the defendants with "a detailed room-by-room inventory of all items seized from the company, including a listing of the various ***297** computers that were imaged." Appellee's Br. at 127. That listing surely offered the defendants some aid in identifying and marshaling the documents relevant to the litigation. Accordingly, we decline to hold that the district court abused its discretion in failing to order the government to produce discovery in a different form.

2. *The Abdication of* Brady

The defendants next argue that the government shrugged off its obligations under *Brady* by simply handing over millions of pages of evidence and forcing the defense to find any exculpatory information contained therein. In essence, the defendants contend that the government was obliged to sift fastidiously through the evidence-the vast majority of which came from Berkeley itself-in an attempt to locate anything favorable to the defense. This argument comes up empty.

In *United States v. Skilling*, 554 F.3d 529 (5th Cir.2009), *vacated in part on other grounds*, --- U.S. ----, 130 S.Ct. 2896, 177 L.Ed.2d 619 (2010), the Fifth Circuit confronted and rejected a nearly identical argument. There, disgraced Enron CEO Jeffrey K. Skilling advanced the following contentions:

> Skilling ... asserts that the government's use of an open file failed to satisfy its *Brady* obligation to disclose material evidence. Skilling contends that the government's open file, which consisted of several hundred million pages of documents, "resulted in the effective concealment of a huge quantity of exculpatory evidence." As the government never directed Skilling to a single *Brady* document contained in the open file, Skilling argues that the government suppressed evidence in violation of *Brady*.
>
> *Id.* at 576.

[12] In dismissing Skilling's argument, the Fifth Circuit noted that, "[a]s a general rule, the government is under no duty to direct a defendant to exculpatory evidence within a larger mass of disclosed evidence." *Ibid.* (citing *United States v. Mulderig*, 120 F.3d 534, 541 (5th Cir.1997)). However, the *Skilling* court added a caveat:

> We do not hold that the use of a voluminous open file can never violate *Brady*. For instance, evidence that the government "padded" an open file with pointless or superfluous information to frustrate a defendant's review of the file might raise serious *Brady* issues. Creating a voluminous file that is unduly onerous to access might raise similar concerns. And it should go without saying that the government may not hide *Brady* material of which it is actually aware in a huge open file in the hope that the defendant will never find it. These scenarios would indicate that the government was acting in bad faith in performing its obligations under *Brady*.
>
> *Id.* at 577.

Here, the government did not engage in any conduct indicating that it performed its *Brady* obligations in bad faith. First, there is no proof that the government larded its production with entirely irrelevant documents. [FN28] Furthermore, it cannot be said that the government made access to the documents *unduly* onerous. While access***298** to the documents may have been somewhat hampered due to the format in which they were transferred, the district court noted that the defendants' motion practice "demonstrate[d] they [were] capably navigating the discovery, which primarily all came from [the] [d]efendants in the first place." [FN29] Finally, there is no indication that the

government deliberately concealed any exculpatory evidence in the information it turned over to the defense.[FN30] Consequently, the government has not "abdicated" its duties under *Brady*.

FN28. The defendants contest this point, noting that the government admitted it did not review everything that it turned over to the defense. However, the fact that the government did not know whether the documents were relevant does not establish that the government intentionally produced irrelevant discovery. Nor is there any indication that the government was willfully blind as to the pertinence of the materials that it was handing over.

FN29. As the government points out, the defendants' ability to peruse the electronic discovery was admitted by the defendants' expert witness at the *Kastigar*-like hearing. Specifically, the witness testified that he was able to sift through the discovery using software called Concordance, which "does a very quick and thorough search ... and tells you how many hits you have, and then tells you how many documents there are associated with that search."

FN30. "If there is something exculpatory still in the [discovery that was produced], we must assume-as there is no compelling evidence to the contrary-that the government does not know about it either." *Skilling*, 554 F.3d at 577.

3. *The Denial of a Continuance*

On December 28, 2007, the defendants requested a 90-day continuance, which would have pushed the commencement of the trial from January 8, 2008 to April 8, 2008. In making the request, the defendants contended that they had been afforded insufficient opportunity to review the evidence, stating: "[i]t is as if the government has pointed the defendants to the Earth's oceans, saying 'there is your discovery.' " The district court declined to grant the request, noting that "[c]ounsel for [the] [d]efendants outnumber counsel for the government, and have all been working on this case for a substantial amount of time." [FN31] The defendants now argue that the district court's denial of their request for a continuance was error.

FN31. The district court also observed that "[t]rial was originally scheduled for November 13, 2007, and the [c]ourt continued it for other reasons than any purported evidentiary problems."

[13][14] The district court's denial of a motion for a continuance is reviewed for abuse of discretion. *United States v. Crossley*, 224 F.3d 847, 854 (6th Cir.2000). "Denial amounts to a constitutional violation only if there is an unreasoning and arbitrary 'insistence upon expeditiousness in the face of a justifiable request for delay.' To demonstrate reversible error, the defendant must show that the denial resulted in actual prejudice to his defense." *United States v. Gallo*, 763 F.2d 1504, 1523 (6th Cir.1985) (quoting *United States v. Mitchell*, 744 F.2d 701, 704 (9th Cir.1984)). "The defendant demonstrates 'actual prejudice' by showing that a continuance would have made relevant witnesses available or added something to the defense." *United States v. King*, 127 F.3d 483, 487 (6th Cir.1997); *see also United States v. Faulkner*, 538 F.2d 724, 729 (6th Cir.1976) ("No absolute rule can be articulated as to the minimum amount of time required for an adequate preparation for trial of a criminal case.").

The defendants argue that they were prejudiced in two ways. First, they argue that "their counsel could not satisfy their constitutional obligation to review all the evidence in the government's possession, custody, or control." [FN32] Appellant's Br. at 60. In making this argument, they allege that "the entirety of the government's ***299** 360,000 pages of trial exhibits ... were largely disclosed on November 29, 2007, only six weeks before trial." *Id.* at 59. Second, the defendants argue that "[t]he defense simply did not have sufficient time to locate and then utilize material and exculpatory evidence that was hidden within the millions of pages of discovery." *Id.* at 60.

FN32. The defendants' attorneys submitted sworn affidavits to this effect, though they point to no authority establishing a "constitutional obligation" to review all evidence in the government's possession.

These arguments lead nowhere. With respect to the first, it must be noted that more than a year elapsed between the time the indictment was handed down and

the time the trial began, affording the defendants ample opportunity to construct a defense.[FN33] Additionally, the discovery time line does not indicate that the defendants were shortchanged with respect to preparation time. The bulk of the documents in question were in the company's possession as early as April 2005.[FN34] Furthermore, the entirety of the discovery material in the case was in the defendants' hands by June 2007, more than six months in advance of the trial. While the government did not provide the defense with thirteen discs of potential trial exhibits until November 29, 2007-approximately six weeks before trial was to begin-those exhibits were ostensibly culled from the discovery material that the government had already provided.[FN35] It is true that this case involved millions of pages of documents, but there is no dispute that the defendants were given months to comb through the bulk of them. As a result, it cannot be said that the district court's unwillingness to postpone the trial was the product of an undue insistence on haste.

FN33. The defendants were indicted in September 2006, and trial commenced in January 2008.

FN34. As mentioned earlier, most of the discovery in this case was obtained from Berkeley computers, which were imaged during the March 2005 search of Berkeley's headquarters. Aside from several laptops which were seized and returned, Berkeley remained in possession of all the imaged computers once the physical search was done. Thus, Berkeley's claim that it had too little time to review the contents of the computers rings hollow.

FN35. Allegedly, two of those discs were corrupted and could not be opened until approximately a week before the trial began. However, that does not change the analysis. Though the defendants were given relatively little time to review the trial exhibits, they were nonetheless given a significant period of time in which to review the discovery materials and prepare their defense.

The defendants' second argument-that they were not given enough time to mine exculpatory evidence from the mountains of discovery dumped at their feet-similarly fails. As an initial matter, it should be noted that this argument assumes that exculpatory evidence exists. In the absence of such evidence, the lack of time to look for it would be harmless. In other words, it would not be prejudicial if the defendants were denied the chance to excavate in a mine that contained no ore. On that score, the most the defendants can say is that they "fervently believe[ ] ... that with sufficient time they would unearth the necessary volume of emails to counter the government's accusations." Appellant's Brief at 60. Consequently, the defendants have failed to demonstrate that the denial of a continuance worked any prejudice with respect to their ability to glean exculpatory evidence. [FN36]

FN36. Furthermore, any emails that the defendants might have found were continuously in their possession from the time of the indictment to the time of the trial. Thus, the defendants had more than a year to turn up anything exculpatory.

D. Warshak's New Trial Motion: *Brady*

[15] The next issue is whether the district court erred in denying **Warshak's** motion***300** for a new trial, which was based on the assertion that the government had suppressed exculpatory evidence in violation of *Brady*. "This court reviews [the] denial of a motion for new trial based on *Brady* violations under an abuse of discretion standard." *United States v. Graham*, 484 F.3d 413, 416 (6th Cir.2007) (citing *United States v. Jones*, 399 F.3d 640, 647 (6th Cir.2005)). "However, the district court's determination as to the existence of a *Brady* violation is reviewed de novo." *Id.* at 416-17 (citing *United States v. Miller*, 161 F.3d 977, 987 (6th Cir.1998)).

[16] "To establish a violation of *Brady*, the [defendant] has the burden of establishing that the prosecutor suppressed evidence; that such evidence was favorable to the defense; and that the suppressed evidence was material." *Carter v. Bell*, 218 F.3d 581, 601 (6th Cir.2000). "[E]vidence is material only if there is a reasonable probability that, had the evidence been disclosed to the defense, the result of the proceeding would have been different. A 'reasonable probability' is a probability sufficient to undermine confidence in the outcome." *United States v. Bagley*, 473 U.S. 667, 682, 105 S.Ct. 3375, 87 L.Ed.2d 481 (1985); *see also Kyles v. Whitley*, 514 U.S. 419, 434, 115 S.Ct. 1555, 131 L.Ed.2d 490 (1995) (holding that the "touchstone

of materiality is a 'reasonable probability' of a different result"). "Moreover, in determining whether undisclosed evidence is material, the suppressed evidence is considered collectively, rather than item-by-item, to determine if the 'reasonable probability' test is met." *Schledwitz v. United States*, 169 F.3d 1003, 1012 (6th Cir.1999).

[17] In this case, the information alleged to constitute *Brady* material was discovered post-trial while **Warshak** was defending himself in a civil action involving the FTC. During that litigation, **Warshak** deposed Sue and Greg Cossman, his sister and brother-in-law, whom the government had interviewed extensively in the run-up to **Warshak's** criminal trial.[FN37] In their depositions, the Cossmans spoke favorably of Berkeley and testified that government investigators were pushing a particular version of the facts. In addition to the depositions, **Warshak's** involvement in the FTC litigation led to the discovery of (1) several recordings of Berkeley sales calls during which disclosure of the auto-ship program was made and (2) several printouts of Berkeley's website on which disclosure of the auto-ship program could be seen. **Warshak** argues that this evidence was exculpatory and should have been turned over prior to trial.

> FN37. Sue Cossman did not testify at **Warshak's** trial. Greg Cossman did, however.

However, **Warshak's** argument fails because the evidence at issue was not "material" for *Brady* purposes. First of all, with respect to Sue Cossman's deposition testimony, it must be noted that, as **Warshak's** sister and a participant in the Berkeley fraud, she had plenty of incentive to stretch the truth in **Warshak's** favor. Furthermore, many of the favorable things she said in her deposition were echoed in the statements of trial witnesses, who stated that they did not realize what they were doing was wrong. Thus, the cumulative nature of her deposition testimony cuts against a finding of materiality. *See Spence v. Johnson*, 80 F.3d 989, 995 (5th Cir.1996) ("[W]hen the undisclosed evidence is merely cumulative of other evidence, no *Brady* violation occurs."). Finally, her testimony would not have undermined confidence in the finding of fraud, as numerous witnesses and scores of emails confirmed that Berkeley executives were engaging in deliberately deceitful practices. *See Jones*, 399 F.3d at 648 ("Given the overwhelming evidence of ***301** guilt, a new trial under *Brady* was inappropriate.").

Greg Cossman's deposition testimony is likewise immaterial. Critically, Greg Cossman took the stand at **Warshak's** trial, at which time he actually made most of the favorable remarks that later appeared in his post-trial deposition.[FN38] For example, Cossman testified at trial that, "while [he] was participating at Berkeley, [he] had no suspicion of participating in a conspiracy doing anything that was criminal." Also, Cossman apparently testified that the government's investigators were "calculating, ruthless, relentless and intimidating." In light of these statements, Greg Cossman's post-trial deposition testimony adds nothing new to the mix, and it therefore does not constitute *Brady* material.

> FN38. For the same reason, we conclude that the information in Greg Cossman's deposition was not suppressed.

Nor can it be said that the tapes and printouts meet the materiality requirement. Though the recorded calls do contain disclosure of the auto-ship program, that fact is not particularly helpful to **Warshak's** case, given the testimony that the disclosures were designed to be ineffective. Similarly, the appearance of the disclosure on the company website at a given instant in time is also unhelpful; there was testimony that the disclosure on the website appeared, shifted, and disappeared like water in the vision of a desert traveler. As a consequence, these materials do not generate a "reasonable probability" of a different result.[FN39] *Kyles*, 514 U.S. at 434, 115 S.Ct. 1555. Accordingly, the district court did not err in finding that **Warshak** failed to demonstrate a *Brady* violation.

> FN39. The calls and website printouts clearly fail to satisfy the suppression requirement as well. There was testimony in the record that Berkeley taped all of its calls, meaning **Warshak** had access to the calls long before the government disclosed the tapes. Furthermore, with respect to the website printouts, it must be noted that they came from *Berkeley's* website. Anything on Berkeley's website should have been known to Berkeley's owner.

E. Prosecutorial Misconduct

The defendants also argue that a new trial is warranted in light of "serious improprieties in the government's rebuttal argument." Appellant's Br. at 69. Specifically, the defendants assert that the following acts constitute reversible misconduct:

> The government's attorney vouched for the "honesty and integrity" of the prosecution team.
>
> The government's attorney expressed his personal opinion with respect to the guilt of the defendants, describing the defendants as "weak" and "self-aggrandiz[ing]."
>
> The government's attorney described his personal life, relating anecdotes about his time in the JAG Corps and his association with a military celebrity.
>
> The government "suggested to the jury that the fact that the grand jury had found probable cause ... was evidence of ... guilt." Appellant's Br. at 72.
>
> The government improperly asserted that the defendants' guilt was supported by evidence that had not been presented during trial.
>
> The government impermissibly argued that the guilty pleas of coconspirators were evidence of a conspiracy.
>
> The government employed rebuttal "to give a second principal closing argument."
>
> Appellant's Br. at 74.[FN40]

FN40. The defense did not immediately object to any of these acts, although it did request a curative instruction after the argument, objecting to the first four sets of remarks made by the prosecutor.

[18] In determining whether a prosecutor's remarks and conduct merit a new ***302** trial,[FN41] this court utilizes a two-part test. *Cristini v. McKee*, 526 F.3d 888, 899 (6th Cir.2008) (citing *Girts v. Yanai*, 501 F.3d 743, 758-59 (6th Cir.2007)). First, we must determine "whether the prosecutor's conduct and remarks were improper." *United States v. Carter*, 236 F.3d 777, 783 (6th Cir.2001) (citing *United States v. Carroll*, 26 F.3d 1380, 1387 (6th Cir.1994)). Second, if the conduct and remarks were improper, "the court must ... consider and weigh four factors in determining whether the impropriety was flagrant and thus warrants reversal." *Ibid.* The four factors are: "(1) whether the conduct and remarks of the prosecutor tended to mislead the jury or prejudice the defendant; (2) whether the conduct or remarks were isolated or extensive; (3) whether the remarks were deliberately or accidentally made; and (4) whether the evidence against the defendant was strong." *Ibid.* Additionally, "[w]hen considering challenges to a prosecutor's statements at trial, we examine those statements within the context of the [entire] trial to determine whether they were prejudicial error." *Cristini*, 526 F.3d at 899 (citing *Girts*, 501 F.3d at 759).

FN41. "Whether statements made by a prosecutor amount to misconduct and whether such statements render a trial fundamentally unfair are mixed questions of law and fact, which we review *de novo*." *United States v. Carson*, 560 F.3d 566, 574 (6th Cir.2009) (citing *United States v. Francis*, 170 F.3d 546, 549 (6th Cir.1999)).

The flagrancy analysis does not necessarily end this court's inquiry. But if the improper statements were not flagrant, reversal of a conviction is warranted only if "1) the proof of the defendant's guilt is not overwhelming; 2) the defense objected to the statements; and 3) the trial judge did not cure the impropriety through an admonishment to the jury." *United States v. Galloway*, 316 F.3d 624, 632 (6th Cir.2003); *see also United States v. Cobleigh*, 75 F.3d 242, 247 (6th Cir.1996).

1. *Were the Prosecutor's Conduct and Remarks Improper?*

The first step in the prosecutorial-misconduct analysis is to determine whether the conduct and remarks at issue were improper. The first set of allegedly inappropriate remarks related to the honesty and moral character of the prosecution team. Responding to a number of comments made during closing arguments for the defendants, the government's attorney, Mr. Kadon, suggested that the defense had labeled the prosecution team "abusive and horrible and evil people." Kadon then stated:

> First of all, I think the biggest thing you heard [during the defense's argument] was that this is a big

> conspiracy, that the conspirators are not seated behind me; the conspirators are seated over there where I am. I mean, I'm a conspirator, I guess; that Ms. Porter, Mr. Josephs, the federal police that have been investigating this case, somehow the Postal Inspection Service, Federal Bureau of Investigation, Food and Drug Administration, the Department of Justice, the United States Attorney's Office and the Criminal Investigation Division of the Internal Revenue Service all got together and conspired, that over the last several years all we thought about every single day when we came to work was how we were going to get these guys.

Kadon then suggested that he "hope[d] [the jury] d[id]n't believe that," and he went on to argue that "it is kind of preposterous that we would all get together and ***303** lie to do this, that this case is somehow worth everything-our reputations, our lives, our families-just because convicting this guy or these people is so important to us."

[19] The defendants contend that these remarks constitute improper prosecutorial vouching, which typically "occurs when a prosecutor supports the credibility of a *witness* by indicating a personal belief in the witness's credibility[,] thereby placing the prestige of the office of the United States Attorney behind that witness." *Francis,* 170 F.3d at 550 (emphasis added). Here, however, Kadon did not vouch for the credibility of a witness. Rather, he spoke to the likelihood that the government's attorneys had engaged in a monomaniacal witch-hunt. Furthermore, he did not overtly suggest that the government's attorneys were honest or morally superior. Instead, he suggested that the prosecution team had no motive to lie. That said, we do think Kadon went a bit overboard, and his remarks veered into dangerous territory.

The next allegedly improper remarks pertained to Kadon's opinion of the defendants. At one point, Kadon posed and then answered the following series of rhetorical questions: "Do I believe that these people were weak, that they sought self-aggrandizement, personal gain, and they sought it at the expense of other people, consumers? And, in fact, it's okay to lie to banks, because who cares about them anyway? Do I believe that they believe that? Yes."

[20] These remarks were also inappropriate. As the defendants correctly note, "it is improper for a prosecuting attorney in a criminal case to state his personal opinion concerning ... the guilt of a defendant." *United States v. Krebs,* 788 F.2d 1166, 1176 (6th Cir.1986) (quoting *United States v. Daniels,* 528 F.2d 705, 709 (6th Cir.1976)); *see also United States v. Bess,* 593 F.2d 749, 755 (6th Cir.1979) ("Implicit in an assertion of personal belief that a defendant is guilty, is an implied statement that the prosecutor, by virtue of his experience, knowledge and intellect, has concluded that the jury must convict. The devastating impact of such 'testimony' should be apparent."). In this case, Kadon plainly voiced a personal belief regarding the guilt of the defendants. While he did not directly state that he believed the defendants were guilty, he stated that, in his mind, they were weak and sought wealth and notoriety at the expense, both literal and figurative, of the consuming public. Thus, Kadon's remarks were improper.

Next, we must consider Kadon's statements about his time in the JAG Corps. In the middle of his summation, Kadon remarked:

> And, you know, when I was on active duty, I worked for a guy named Gary Harrell, who-he was kind of a famous guy. If you have ever seen the movie Black Hawk Down, he was in the movie Black Hawk Down. He's a Green Beret. And he would always tell me when we talked about things-I was his JAG officer, but I don't fly Black Hawks-he would always say, you know, Karl, life is full of choices. You make your choices and accept the consequences, about the things that we were doing with respect to prosecuting the war on terror.

The defendants argue that the prosecutor's remarks about his military service and his quasi-famous colleague were improper. With respect to these remarks, the government concedes impropriety, acknowledging that the remarks were entirely irrelevant to the closing argument. We agree. The remarks served no purpose other than to enhance Kadon's stature in the eyes of the jury, and they were therefore inappropriate. This conclusion is especially***304** apparent when one considers the good guys/bad guys dichotomy that the remarks create when paired with Kadon's statements regarding the "weakness" and cupidity of the defendants.

The fourth set of statements at issue touched on the relevance of the grand jury's decision to indict the

defendants. Following his comments about his stint in the armed forces, Kadon noted that all 112 counts in the indictment were "things that a grand jury determined were probable cause, these people committed these crimes, that's what that means." Sometime thereafter, Kadon returned to the mindset of the grand jury, stating that "[t]he grand jury believed [the defendants] committed crimes."

[21] These remarks were plainly out of bounds. As this court stated in *Bess*, "it is always improper for a prosecutor to suggest that a defendant is guilty merely because he is being prosecuted or has been indicted." 593 F.2d at 754; *see United States v. Bowen*, 500 F.2d 41, 42 (6th Cir.1974) (holding that it was improper for a prosecutor to state that an eyewitness identification "was good enough" when it was presented to the grand jury). Here, there is no question that Kadon invoked the grand jury's probable-cause determination when arguing for a finding of guilt. His remarks were therefore improper.

The fifth set of remarks at issue involved individuals who had filed complaints but had not testified at trial.[FN42] First, Kadon stated that, despite floods of complaints to Berkeley and the BBB, the government had made a strategic decision not to "bring[ ] in a million people or hundreds of thousands of people" to testify that Berkeley was shipping them unwanted supplements. Then, Kadon remarked that thousands of callers had unsuccessfully attempted to call Berkeley and that the government did not "have to go and have everyone here say: I called; it was a problem."

> FN42. It should be noted that because the defendants did not object to these statements below, they are subjected to review for plain error. *See Cristini*, 526 F.3d at 901. Ultimately, however, the level of review is irrelevant, as the remarks were not improper.

The defendants argue that these comments impermissibly "convey[ed] the impression that evidence not presented to the jury, but known to the prosecutor, support[ed] the charges against the defendant[s] and ... thus jeopardize[d] the defendant[s'] right to be tried solely on the basis of the evidence presented to the jury." *Hodge v. Hurley*, 426 F.3d 368, 378 (6th Cir.2005). However, the defendants are incorrect. The remarks in question merely alluded to evidence already before the jury, namely, testimony that droves of customers had complained and that scores of others had tried in vain to do the same. In suggesting that those witnesses could have testified, the government was simply explaining their absence. As a result, these remarks were permissible.

The penultimate allegation of prosecutorial impropriety stems from a remark about the coconspirators who testified at trial.[FN43] Specifically, Kadon stated: "And if you believe that there was an agreement to put this on between the people here at the table, the ones who were charged and the people that testified, they pled guilty to doing that, that's one part of the conspiratorial element right there, those people."

> FN43. As with the previous set of remarks concerning potential witnesses, this comment did not spur an objection at trial and is therefore subject to plain-error review.

[22] This declaration was not improper. While it is true that a jury "may not ***305** ... consider the guilty plea of any [other] person as evidence of guilt on the part of the defendant [standing trial]," *United States v. Stavroff*, 149 F.3d 478, 484 (6th Cir.1998), Kadon's remark did not directly implore the jurors to consider the guilty pleas of the defendants' coconspirators. Instead, Kadon simply added an identifier as to whom the charged defendants were shown to have conspired with-a number of other defendants who had pleaded guilty. That portion of his statement did not lie at the core of the message he was intending to convey, which was that the jurors should convict if they found the existence of a conspiratorial agreement. Consequently, Kadon's statement should not be deemed inappropriate. [FN44]

> FN44. Even if it were deemed improper, the third of the four flagrancy factors-whether the remark was deliberate or accidental-would militate against a finding that this remark was particularly pernicious. Kadon's statement was clearly a spontaneous aside that, in fact, interrupted the flow of the main point he was trying to make.

Lastly, the defendants argue that Kadon engaged in improper conduct, specifically by employing the government's rebuttal argument as an impermissible second attempt at a full-scale closing. The defendants

contend that the government deliberately limited its initial closing argument to a "45-minute long [sic] broad-brush overview of its evidence, and withheld many of its most pointed arguments for rebuttal." Appellant's Br. at 75.

[23] However, the defendants' argument fails. True, a number of cases suggest that the government may not advance any new contentions on rebuttal. *See, e.g., United States v. Gleason,* 616 F.2d 2, 26 (2d Cir.1979) (indicating that prejudice might have arisen if a rebuttal argument containing new assertions had not been followed by surrebuttal). However, the defendants point to nothing in Kadon's rebuttal argument that was raised for the first time after their summation. Furthermore, to the extent that Kadon made any new arguments in response to assertions made by the defense, those new arguments were permissible. *See United States v. Sarmiento,* 744 F.2d 755, 765 (11th Cir.1984).

2. *The Four Flagrancy Factors*

[24] Having determined that a number of Kadon's remarks were improper, we must now proceed to the flagrancy analysis, which involves the application of the four factors delineated above. None of the four factors is dispositive. *Galloway,* 316 F.3d at 632. On balance, it appears that the prosecutor's remarks, though improper, were not flagrant enough to "render [the] trial fundamentally unfair." *Carson,* 560 F.3d at 574.

a. *Tendency to Mislead the Jury or Prejudice the Jury*

The first factor requires us to consider whether the remarks in question were misleading or prejudicial. *Carter,* 236 F.3d at 783. As an initial matter, it must be noted that the defendants did not *immediately* object to any of the remarks. In some cases, the defendants did not object at all. That cuts in favor of a finding that the remarks were not particularly prejudicial, as anything significantly deleterious would presumably prompt a swift objection from experienced defense counsel. *See United States v. Trutenko,* 490 F.2d 678, 680 (7th Cir.1973) ("We are inclined to believe[,] however, that if the comment were sufficiently prejudicial to warrant reversal, counsel who was present at the time either would have objected forthwith or else would have requested the trial judge to ***306** give a curative instruction.").[FN45]

FN45. As noted in footnote 40, the defense did request a curative instruction following the argument, objecting to all of the remarks at issue, save those about additional evidence and the guilty pleas of co-defendants. But the request for a curative instruction does not alter the analysis in any great respect. If veteran trial counsel failed to interrupt the argument, then counsel must have been of the opinion that a somewhat delayed curative instruction would suffice to extinguish any prejudice. This assertion finds corroboration in the mystification of the trial judge, who was somewhat perplexed when the defendants presented objections after Kadon had concluded his rebuttal and asked, "Why didn't you object at the time?"

Setting aside the failure to lodge an immediate objection, it seems evident that a number of the improper remarks would tend, in isolation, to prejudice the defendants. The perceptions of the jury were surely impacted to some extent when the prosecutor suggested that he believed the defendants to be weak, greedy, and capable of criminal designs. *See Bess,* 593 F.2d at 755. Furthermore, it is plain that Kadon's military anecdote was likely to stir the patriotic fibers of at least several jurors, shifting their focus, if only slightly, away from the critical issue of whether the defendants were actually guilty. In addition, the defendants were surely injured when Kadon suggested that the grand jury had formed an opinion as to their guilt. *See Bess,* 593 F.2d at 754 (indicating that a prosecutor commits an "egregious" error when he opines that "a defendant is guilty merely because he ... has been indicted"). Thus, in a vacuum, Kadon's remarks would appear to entail a certain measure of prejudicial force.[FN46]

FN46. With respect to Kadon's remarks about the honesty and moral uprightness of the prosecution team, we note that those remarks were invited by the defense and therefore minimally prejudicial. Indeed, the defendants' attorneys implied on several occasions that the prosecution was ruthless and prized victory in the court over justice in the land. At one juncture, attorneys for the defense stated, "A federal prosecution is supposed to be a search for the truth. It is not a quest to win at all costs on the part of the Department of Justice." Given such remarks,

> the prejudice resulting from Kadon's replies-which sought to counter the notion of corruption within the prosecution team-was plainly minimized because the jury would have "underst[ood] that the prosecutor was countering defense counsel's repeated attacks on the prosecution's integrity." *United States v. Young*, 470 U.S. 1, 17-18, 105 S.Ct. 1038, 84 L.Ed.2d 1 (1985).

However, to the sting of potential prejudice was applied the salve of forceful curative instructions. Once closing arguments were completed, and following a brief recess, the district court warned the jurors that the closing arguments were not evidence. The district court also stated, "[I]t is not appropriate for the lawyers ... to express a personal opinion about the truthfulness of a witness' testimony. That is for you to decide." In addition, the district court commanded the jurors to "disregard any personal opinions or personal backgrounds of counsel." The district court also touched on the issue of Kadon's references to the grand jury. In light of these ameliorative instructions, any prejudice precipitated by Kadon's comments was either extinguished entirely or diminished drastically. *See Carson*, 560 F.3d at 576 (holding that "any prejudice resulting from the comments was 'cured, or at least minimized, by curative instructions to the jury' "); *Carter*, 236 F.3d at 787 ("Ordinarily, a court should not overturn a criminal conviction on the basis of a prosecutor's comments alone, especially where the district court has given the jury an instruction that may cure the error.").[FN47] Accordingly,***307** the first factor does not cut in favor of the defendants.

> FN47. The defendants argue that any remediation achieved by the curative instructions was "too little and too late." Appellant's Br. at 77. However, this assertion is essentially toothless, as the defendants themselves remained mum until the government's attorney had concluded his remarks. If the prosecutor were truly wreaking havoc and casually tossing around indelibly prejudicial remarks, the attorneys for the defense would have vehemently objected, which they were clearly adept at doing during all other phases of the trial.

b. *Isolated v. Extensive*

The second factor requires this court to assess the pervasiveness of the improper remarks; that is, this court must determine whether the remarks were isolated or extensive. "If a prosecutor's comments were simply isolated remarks made during the course of a long trial, then the error caused by such misconduct may be harmless." *Carter*, 236 F.3d at 788 (citing *United States v. Leon*, 534 F.2d 667, 679 (6th Cir.1976)).

In this case, it is tempting to describe the remarks as isolated, as they were confined to a single portion of the trial. Indeed, when the remarks are viewed-as they must be-against the backdrop of the trial as a whole, they are certainly fairly localized. *See Macias v. Makowski*, 291 F.3d 447, 453 (6th Cir.2002) ("The prosecutor's statement took place during rebuttal closing argument, and Macias does not contend that the prosecutor acted inappropriately at any other point during the trial. Because the comments were isolated, this factor does not weigh in Macias's favor."); *Cobleigh*, 75 F.3d at 247 (holding that there was no prosecutorial misconduct where the defendants complained of "a few unrelated statements and events from an eight-defendant trial that lasted one month and involved the testimony of dozens of witnesses and the presentation of more than 200 exhibits"). However, the fact that the remarks were confined to the rebuttal argument does not mean that they are sufficiently isolated to merit a finding of harmlessness. In some instances, a single forbidden comment is sufficient to poison the entire trial. *See United States v. Smith*, 500 F.2d 293, 297 (6th Cir.1974) ("[E]ven a single misstep on the part of the prosecutor may be so destructive of the right of the defendant to a fair trial that reversal must follow." (citation and internal quotation marks omitted)). Ultimately, we think the remarks, though confined to the rebuttal argument, were numerous enough to escape categorization as isolated. But, at the same time, the remarks were not plentiful enough to merit a finding that they were pervasive. Thus, the second factor is a wash.

c. *Deliberate v. Accidental*

Next, this court must consider whether the remarks were deliberate or accidental. *Carter*, 236 F.3d at 783. Here, only two sets of allegedly improper remarks appear to have been deliberate-the statements regarding the good intentions of the prosecution team and the statements regarding Kadon's experiences as a JAG officer. The remaining remarks appear to have been made on the spur of the moment, sometimes

coming in the middle of wholly unrelated sentences. As a consequence, it does not appear that either side benefits tremendously from this factor. In any event, the prosecutor's intent in making certain remarks is a fairly rough proxy for the ultimate question, which is whether the remarks at issue contaminated the trial with unfairness.

d. *Strength of the Evidence*

The final factor is the strength of the evidence. *Ibid.* In this case, the force of the government's evidentiary presentation weighs heavily against a finding of flagrancy. The government introduced the testimony***308** of multiple Berkeley executives, each of whom testified that the company knowingly attempted to deceive its customers. The executives also testified that the company was manipulating its financial information in order to remain in relationships with its banking partners. The case against the defendants also included copious emails. In short, the evidence against the defendants was extensive. Thus, the fourth and final factor militates in favor of the conclusion that Kadon's remarks, though imprudent, were ultimately harmless. Accordingly, we hold that, on balance, Kadon's improper comments did not rise to the level of flagrancy.

3. *Reversal For Non-Flagrant Remarks*

[25] As noted above, a holding that the remarks at issue were non-flagrant does not put the analysis to rest. Reversal is nonetheless appropriate if three conditions are met: (1) the evidence against the defendants was not overwhelming; (2) the defendants objected to the prosecution's remarks; and (3) the district court failed to issue a curative instruction. *See Galloway,* 316 F.3d at 632. Here, only one of the prerequisites was met: the defendants objected to several of the improper remarks. However, the evidence against the defendants was strong, and the district court offered a curative instruction. Thus, reversal under *Galloway* is not appropriate.

F. Conspiracy to Commit Mail, Wire, & Bank Fraud (18 U.S.C. § 1349)

[26][27] **Warshak** and Harriet contend that the evidence was insufficient to establish the existence of a conspiracy to commit mail, wire, and bank fraud. In reviewing the sufficiency of the evidence, the relevant question is "whether, after viewing the evidence in the light most favorable to the prosecution, *any* rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt." *Jackson v. Virginia,* 443 U.S. 307, 319, 99 S.Ct. 2781, 61 L.Ed.2d 560 (1979). "A defendant challenging the sufficiency of the evidence bears a very heavy burden." *United States v. Prince,* 214 F.3d 740, 746 (6th Cir.2000) (citation and internal quotation marks omitted). "[W]e will reverse a judgment for insufficiency of evidence only if, viewing the record as a whole, the judgment is not supported by substantial and competent evidence." *United States v. Blakeney,* 942 F.2d 1001, 1010 (6th Cir.1991) (citing *United States v. Ellzey,* 874 F.2d 324, 328 (6th Cir.1989)).

[28][29][30] "A conviction for conspiracy to commit ... fraud requires proof beyond a reasonable doubt that the defendant knowingly and willfully joined in an agreement with at least one other person to commit an act of ... fraud and that there was at least one overt act in furtherance of the agreement." *United States v. Cantrell,* 278 F.3d 543, 546 (6th Cir.2001) (citing *Crossley,* 224 F.3d at 856). "Circumstantial evidence that a reasonable person could interpret as showing participation in a common plan may be used to establish the existence of a conspiracy agreement." *Ibid.* Furthermore, "a conspiracy to achieve two or more unlawful goals, in the conjunctive, can properly be supported by proof of any of the alleged goals." *United States v. Thomas,* 54 F.3d 73, 81 (2d Cir.1995) (citing *Griffin v. United States,* 502 U.S. 46, 56-57, 112 S.Ct. 466, 116 L.Ed.2d 371 (1991)).

1. ***Warshak***

[31] **Warshak** argues that the government failed to satisfy its burden of proof in several respects. First, he argues that, even if the government proved that a conspiracy existed, the government's proof was insufficient to show that the conspiracy***309** lasted for the entirety of the period alleged in the indictment. Second, **Warshak** argues that there was simply no proof that he entered into a conspiracy to commit mail, wire, and bank fraud. He argues that all of the practices that the government labeled fraud were simply the missteps of a fledgling business attempting to find its footing while simultaneously experiencing radical growth. Third, he argues that there was no conspiracy to commit bank fraud as the chargeback-manipulation efforts were never intended to harm a bank. All three of these arguments fail.[FN48]

FN48. **Warshak** also alleges that his conviction on Count 1 should be reversed be-

cause the district court permitted the jury to convict him on a legally erroneous theory of bank fraud. As explained *infra* in Part II.H, this argument also fails.

[32] **Warshak's** first argument is a non-starter. While the indictment did allege a conspiracy lasting from 2001 to 2006, the government was under no obligation to prove that the conspiracy spanned the entirety of that time frame. As the Tenth Circuit explained in *United States v. Henderson*, "the temporal scope of a conspiracy is not an 'essential' or 'material' element of the charge." 179 Fed.Appx. 535, 538 (10th Cir.2006) (quoting *United States v. Cina*, 699 F.2d 853, 859 (7th Cir.1983)); *see United States v. Davis*, 679 F.2d 845, 852 (11th Cir.1982) ("Neither is time an essential element so long as the time frame proved was within the period alleged in the indictment.") (citing *Russell v. United States*, 429 F.2d 237, 238 (5th Cir.1970)). Thus, the evidence was sufficient so long as the government proved a conspiracy within the relevant chronological bounds.

And the government did. Though **Warshak** claims that his company's early practices were the result of his status as a managerial neophyte, and that the company later took corrective measures to ensure that any deceptive practices were remediated, a reasonable juror could nonetheless conclude that **Warshak** and his associates conspired to defraud both customers and merchant banks. As a number of former Berkeley executives testified, the existence of the auto-ship program was not disclosed to customers for the first year that Berkeley was in business, leading to scores of unauthorized credit-card transactions. Furthermore, though disclosures were eventually made during sales calls, the disclosures were designed to fail. They were made at the end of the calls and came on the heels of information relating to sexually transmitted diseases. A reasonable juror could easily conclude that any supposedly remedial measures were simply undertaken to create plausible deniability. As a result, there was sufficient evidence to support the conclusion that the defendants conspired to commit mail and wire fraud.[FN49] Under *Thomas*, that is enough to sustain a conviction on Count 1. *See* 54 F.3d at 81 (holding that proof of any single illegal aim of the conspiracy is sufficient to sustain a conviction).

FN49. Additionally, a reasonable juror could conclude that the conspiracy lasted for the entirety of the period alleged in the indictment. While the supposed remedial measures took place in 2004, those remedial measures were, according to testimony, merely for show. Thus, one could conclude that any business conducted after disclosures were instituted was part and parcel of an ongoing scheme to defraud customers.

A reasonable juror could also conclude that the defendants conspired to commit bank fraud. Though **Warshak** argues that the chargeback-manipulation scheme was not intended to harm any banks, a reasonable juror could nonetheless conclude that the scheme was concocted and implemented***310** with fraudulent intent. According to a number of Berkeley insiders, **Warshak** and his employees manipulated the chargeback ratio because, if they did not, their merchant accounts would be terminated. Thus, a reasonable juror could find that the intent of the chargeback-manipulation scheme was to deceive merchant banks (and credit-card processors) into continuing to provide a service that they would otherwise have declined to provide. That action would constitute fraud by increasing a risk of loss, even if no actual monetary loss were shown. *United States v. Reaume*, 338 F.3d 577, 581 (6th Cir.2003). Consequently, there was sufficient evidence to support the conclusion that **Warshak** and the other named defendants conspired to commit bank fraud.[FN50]

FN50. Testimony that the defendants submitted a number of falsified applications to banks and processors was also offered in support of the conspiracy charge. However, because the evidence relating to the chargeback scheme was sufficient to sustain a conviction, any evidence relating to the applications need not be discussed.

2. *Harriet*

[33] Harriet argues that the evidence was insufficient to prove that she knowingly joined the conspiracy. She argues that, although she was in charge of processing continuity shipments at Berkeley, her job amounted to little more than pushing a button. In addition, she contends that she was not made privy to any emails discussing the auto-ship program or the chargeback ratio. In sum, she asserts that she was oblivious to any fraud that was occurring at the company and that she was convicted simply by virtue of

her name.

However, there is competent evidence in the record suggesting that Harriet was a knowing participant in the pervasive fraud at Berkeley. According to Shelley Kinmon, Harriet was used to input auto-ship charges because she was the only one **Warshak** trusted. Furthermore, there is testimony that Harriet was present at staff meetings where the need to manipulate the chargeback ratio was discussed. From this evidence, a rational factfinder could properly determine that Harriet knowingly joined the conspiracy.[FN51]

FN51. There is also evidence linking Harriet to the falsified bank applications.

G. Mail Fraud (18 U.S.C. § 1341)

[34] **Warshak** also argues that the government failed to offer sufficient evidence that he was guilty of the twelve mail-fraud counts alleged in the indictment (Counts 2-13). "Mail fraud [under 18 U.S.C. § 1341] consists of (1) a scheme or artifice to defraud; (2) use of mails in furtherance of the scheme; and (3) intent to deprive a victim of money or property." *United States v. Turner*, 465 F.3d 667, 680 (6th Cir.2006). Notably, "the mail ... fraud statute[ ] do[es] not require proof that the intended victim was actually defrauded; the actual success of a scheme to defraud is not an element of ... § 1341...." *United States v. Merklinger*, 16 F.3d 670, 678 (6th Cir.1994). Indeed, "[u]sing the mail to execute or attempt to execute a scheme to defraud is indictable as mail fraud ... even if no one relied on any misrepresentation." *Bridge v. Phoenix Bond & Indem. Co.*, 553 U.S. 639, 648, 128 S.Ct. 2131, 170 L.Ed.2d 1012 (2008) (citing *Neder v. United States*, 527 U.S. 1, 24-25, 119 S.Ct. 1827, 144 L.Ed.2d 35 (1999)).

[35] The first element of mail fraud, the requirement of a "scheme or artifice to defraud," escapes precise definition. In *United States v. Daniel*, we held that " '[a] scheme to defraud includes any plan or course of action by which someone intends to deprive another by deception of money ***311** ... or property by means of false or fraudulent pretenses, representations, or promises.' " 329 F.3d 480, 485 (6th Cir.2003) (quoting *United States v. Gold Unlimited, Inc.*, 177 F.3d 472, 479 (6th Cir.1999)). However, we have acknowledged that the "scheme to defraud element required under § 1341 is not defined according to a technical standard. The standard is a 'reflection of moral uprightness, of fundamental honesty, fair play and right dealing in the general and business life of members of society.' " *United States v. Van Dyke*, 605 F.2d 220, 225 (6th Cir.1979) (quoting *United States v. Bruce*, 488 F.2d 1224, 1229 (5th Cir.1973)).

Mail fraud's second element, the requirement of a mailing in furtherance of the scheme, is also fairly expansive. *See United States v. Wood*, 364 F.3d 704, 726 (6th Cir.2004) ("[T]he Supreme Court has minimized the importance of mailings in establishing a mail fraud offense[.]"). As the Supreme Court noted in *Schmuck v. United States*, "[t]he relevant question ... is whether the mailing is part of the execution of the scheme as conceived by the perpetrator at the time." 489 U.S. 705, 715, 109 S.Ct. 1443, 103 L.Ed.2d 734 (1989). "[T]he use of the mails need not be an essential element of the scheme." *Id.* at 710, 109 S.Ct. 1443 (citing *Pereira v. United States*, 347 U.S. 1, 8, 74 S.Ct. 358, 98 L.Ed. 435 (1954)). Rather, "[i]t is sufficient for the mailing to be incident to an essential part of the scheme, or a step in the plot." *Id.* at 710-11, 109 S.Ct. 1443 (internal citation and quotation marks omitted). "Those who use the mails to defraud proceed at their peril." *Id.* at 715, 109 S.Ct. 1443.

In the present case, the mail-fraud charges involved specific customers who ordered a free trial of some Berkeley product-whether over the phone, online, or through the mail-and thereafter received an unwanted (and unauthorized) additional shipment. In a number of cases, the customers were never informed during the ordering process that they would be charged for anything beyond the shipping-and-handling costs associated with the trial offer. In other cases, customers were notified that they would be receiving additional shipments and incurring additional charges, but those customers were also told that they could remove themselves from the auto-ship program within a certain period of time. Those customers later attempted to cancel their enrollment in the program but were unsuccessful, some despite receiving confirmation numbers. In addition, the majority of the customers, including those to whom disclosure was not made, reported encountering great difficulty in obtaining a refund.

Warshak argues that there was insufficient evidence to support his convictions on these charges, as the government failed to demonstrate the existence of an intentional scheme to defraud. Appellant's Br. at 102-10. **Warshak** notes that, in some cases, the cus-

tomers involved were aware that they had been enrolled in the auto-ship program. **Warshak** also notes that a number of customers were able to obtain full or partial refunds. He contends that, at best, the evidence shows a number of "classic dispute[s] between company and customer." Appellant's Br. at 108. He also posits that a number of the shipments at issue might be attributable to individual mistakes on the part of telephone operators.

But **Warshak** misses the point. The government's theory was that Berkeley's method of doing business was deliberately geared toward deceiving customers into purchasing additional supplements through the auto-ship program, and there was certainly sufficient evidence for a reasonable juror to conclude that the government's theory was correct. At trial, James Teegarden***312** testified that the auto-ship program was the "life blood" of the company and that no pre-sale disclosure of the auto-ship program was made in the early stages of the business. Both Teegarden and Shelley Kinmon testified that, while disclosures were later implemented after the company was inundated with complaints, the disclosures were designed to be ineffective because nobody would sign up for continuity if it were properly described. Thus, it is reasonable to conclude that Berkeley's whole sales operation was simply one gargantuan scheme to defraud. Whether the individual consumers named in the mail-fraud counts were actually deceived is immaterial; the success of the scheme is not an essential element of mail fraud. *See Bridge,* 553 U.S. at 648, 128 S.Ct. 2131; *Merklinger,* 16 F.3d at 678. All that matters is that the customers were the targets of an intentional scheme to defraud, and there is certainly sufficient evidence for a reasonable juror to conclude that they were.

Additionally, there is sufficient evidence to establish the mailing element of the offense. Each of the customers testified that he or she received an additional, unwanted shipment of herbal supplements through the mail. Without those shipments, Berkeley would have had absolutely no justification for placing additional charges on its customers' credit cards. Only with the subsequent shipments could Berkeley even begin to create the illusion that the unauthorized charges were legitimate. Thus, the shipments plainly satisfy the mailing requirement, as they were clearly "part of the execution of the scheme." *Schmuck,* 489 U.S. at 715, 109 S.Ct. 1443.

H. Bank Fraud (18 U.S.C. § 1344)

1. *The Jury Instructions*

[36] The defendants' first argument is that the district court's instructions permitted the jury to convict them under a legally erroneous theory of bank fraud. "We review a jury instruction to determine 'whether the charge, taken as a whole, fairly and adequately submits the issues and applicable law to the jury.' " *United States v. Hoglund,* 178 F.3d 410, 412 (6th Cir.1999) (quoting *United States v. Martin,* 740 F.2d 1352, 1361 (6th Cir.1984)).

[37] To obtain a conviction for bank fraud under 18 U.S.C. § 1344, the government must demonstrate three elements: "(1) that the defendant knowingly executed or attempted to execute a scheme to defraud a financial institution; (2) that the defendant did so with the intent to defraud; and (3) that the financial institution was insured by the FDIC." *United States v. Everett,* 270 F.3d 986, 989 (6th Cir.2001).

At trial, the district court instructed the jury that the government could demonstrate the requisite intent to defraud (*i.e.,* the second element of the offense) in "several different ways," and stated that "it is not necessary that a bank be the intended target of the fraud." The district court also suggested that "the government can ... show that the defendant had the requisite intent to defraud, even if the intended target ... was a third party, if it proves ... that: (1) the defendant exposed a bank to risk of loss or intended to do so; or (2) caused the bank to transfer funds that were in its possession or control."

The defendants argue that these instructions were improper because they allowed the jury to convict on the basis of an intent to defraud the credit-card processors, as opposed to an intent to defraud the merchant banks. The defendants contend that the language of the bank-fraud statute clearly requires that any fraudulent scheme "be directed at an *FDIC-insured* ***313** *bank* and not at any other entity or person." [FN52] Appellant's Br. at 112. In support of their contention, the defendants point to several out-of-circuit decisions holding that, to prove bank fraud, the government must show that the defendant intended to defraud the bank itself or that the defendant intended to harm the bank. *See, e.g., United States v. Leahy,* 445 F.3d 634,

647 (3d Cir.2006) ("[W]here there is no evidence that the perpetrator had an intent to victimize the bank, ... an intent to victimize some third party does not render the conduct actionable under § 1344."); *United States v. Laljie,* 184 F.3d 180, 189-90 (2d Cir.1999) ("[A] conviction under § 1344 is not supportable by evidence merely that some person other than a federally insured financial institution was defrauded in a way that happened to involve banking, without evidence that such an institution was an intended victim.").

> FN52. It is conceded that the merchant banks were FDIC-insured.

[38] But the state of the law is different in this circuit. In *Everett,* we definitively held that "to have the specific intent required for bank fraud the defendant need not have put the bank at risk of loss in the usual sense or intended to do so." 270 F.3d at 991. Rather, "[i]t is sufficient if the defendant in the course of committing fraud on *someone* causes a federally insured bank to transfer funds under its possession and control." *Ibid.*; *see United States v. Reaume,* 338 F.3d 577, 581 (6th Cir.2003) (" *Everett* ... can be said to stand for the proposition that the bank fraud statute is violated, even if the intended victim of the fraudulent activity is an entity other than a federally insured financial institution, when the fraudulent activity causes the bank to transfer funds."). In *Reaume,* this court extended the principle articulated in *Everett,* "find[ing] that intent to defraud the federally insured institution itself is satisfied where: (1) the intent to defraud some entity was present; and (2) that intended fraud placed a federally insured financial institution at a risk of loss." 338 F.3d at 582.

Accordingly, it is clear that the district court's instructions did not misstate the law. In the Sixth Circuit, a defendant may be convicted of bank fraud if he intends to defraud someone and implements a fraudulent scheme that either causes a federally insured financial institution to transfer funds or exposes that institution to some degree of risk.

2. *Constructive Amendment/Prejudicial Variance*

[39] Next, the defendants argue that the district court's instructions, when coupled with the government's evidentiary presentation, resulted in a constructive amendment to the indictment. "Constructive amendments ... occur [ ] when an indictment's terms are effectively altered by the presentation of evidence and jury instructions that 'so modify essential elements of the offense charged that there is a substantial likelihood the defendant [was] convicted of an offense other than that charged in the indictment.' " *United States v. Combs,* 369 F.3d 925, 936 (6th Cir.2004) (quoting *United States v. Hathaway,* 798 F.2d 902, 910 (6th Cir.1986)).

Here, no constructive amendment occurred. The offense charged in the indictment was bank fraud, and the district court's instructions did not add any elements extrinsic to that offense. *Cf. Combs,* 369 F.3d at 936 (holding that a constructive amendment had occurred where the jury instructions mixed elements of two distinct offenses). Indeed, the instructions simply clarified that one of the familiar elements of bank fraud-***314** namely, intent to defraud-could be shown through proof of intent to defraud a third party. Thus, it cannot be said that there is a substantial likelihood that either of the defendants was convicted of an uncharged offense.[FN53]

> FN53. The defendants do not argue that the counts improperly mixed the language of § 1344(1) with the language of § 1344(2). If the defendants did, however, such an argument would be fruitless, as the counts charged both offenses in the conjunctive. Furthermore, the district court appears to have given a jury unanimity instruction.

Nor was there a prejudicial variance. A variance takes place "when the charging terms of an indictment are left unaltered, but the evidence offered at trial proves facts materially different from those alleged in the indictment." *United States v. Ford,* 872 F.2d 1231, 1235 (6th Cir.1989) (quoting *Gaither v. United States,* 413 F.2d 1061, 1071 (D.C.Cir.1969)). For a variance to merit reversal, it must be prejudicial-that is, it must detrimentally affect the ability of the defendants to defend themselves. *Hathaway,* 798 F.2d at 910-11 (quoting *United States v. Miller,* 471 U.S. 130, 138 n. 5, 105 S.Ct. 1811, 85 L.Ed.2d 99 (1985)).

In this case, the facts proved at trial were entirely congruent with the facts delineated in the indictment. The bank-fraud counts alleged that the defendants misled merchant banks and credit-card processors about the chargeback ratio. At trial, the government introduced evidence to the same effect. Additionally, the bank-fraud counts alleged that the defendants

submitted falsified applications to numerous merchant banks and credit-card processors for the purpose of establishing merchant accounts. Again, the evidence proffered at trial corresponded with the allegations. It is therefore plain that no variance occurred.

3. *Sufficiency of the Evidence*

[40] Lastly, the defendants argue that the evidence adduced at trial was insufficient to support their bank-fraud convictions (Counts 15, 23, & 27). In each of the bank-fraud counts, the defendants were charged with scheming to defraud a merchant bank in two ways. First, they were alleged to have "falsely inflated the number of sales transactions in order to cause the corresponding ratio of credit card chargebacks from disputed credit card charges to appear lower than, in fact, it was." Second, they were alleged to have submitted falsified applications to obtain credit-card processing services from merchant banks and processors.[FN54]

> FN54. Because the evidence was sufficient to sustain convictions for the charge-back-manipulation scheme, we have omitted discussion of the allegedly falsified applications. It should be noted, however, that the jury failed to convict the defendants of a number of other charges related to the merchant applications. Specifically, the jury acquitted the defendants of making false statements to a bank, in violation of 18 U.S.C. § 1014.

The defendants argue that the government failed to prove that the manipulation of the chargeback ratio caused any of the merchant banks to transfer funds. The defendants claim that "[t]here was ... no testimony from any banker or processor that any bank ever transferred money to Berkeley, nor were any bank, processor, or customer account records introduced reflecting such a transfer." Appellant's Br. at 114-15. The defendants claim that the testimony instead showed that "the *processors* transferred Berkeley's own credit card proceeds to Berkeley, subtracting any transaction fees and chargeback penalties or reserves from the operating revenues." *Id.* at 115 (emphasis added). In short, the ***315** defendants claim that there was "*no* evidence that the banks lost access to any of their funds for any period of time whatsoever." *Ibid.*

However, there is evidence in the record suggesting the that the merchant banks did indeed transfer funds as a result of the chargeback-manipulation scheme. According to Hector Rodriguez, who managed VISA's chargeback-monitoring program, credit-card processing relationships inherently require merchant banks to transfer funds. In other words, if a credit-card transaction is processed, money flows through a merchant bank. There appears to be some question as to whether the money goes directly into the hands of the merchant, but the record clearly indicates that the merchant bank is at the very least integral to the transfer-it debits the card holder's account and credits someone.[FN55] Therefore, if Berkeley's merchant accounts had been terminated, the merchant banks would no longer have made transfers on the company's behalf. As a number of witnesses testified, without the chargeback scheme, the company's merchant accounts would have been terminated. Thus, a reasonable juror could easily conclude that the fraudulent scheme caused merchant banks to continue to release money under their control.

> FN55. For example, Mike Wagner testified as follows: "Well, the processor didn't actually hold the money. It was just the transition, the actual mechanics of seeing if the credit card was valid to then, perhaps, issue the money, if it was an approved credit card. So if my credit card balance-my credit card is good, for example, I would get an approval at the processor, which would then relay to the merchant bank to give the money, take the money off of my credit card."

The defendants also argue that the evidence was insufficient to show that the chargeback-manipulation scheme exposed the merchant banks to a risk of loss. As an initial matter, it should be noted that, since there is sufficient evidence to show that the merchant banks transferred funds under their control, the conviction may be sustained even if the government failed to prove that the banks took on risk as a result of the scheme. *See* Everett, 270 F.3d at 991; *see also* Mehul Madia, Comment, *The Bank Fraud Act: A Risk of Loss Requirement?*, 72 U. Chi. L.Rev. 1445, 1452-53 (2005) ("The Sixth, Ninth, and Eleventh Circuits have all held that a risk of loss requirement is not necessary for conviction under [§ 1344].").

Nonetheless, there is competent evidence in the record indicating that the efforts to depress Berkeley's

chargeback ratio saddled the merchant banks with risk. First of all, there was abundant testimony that the merchant banks provided Berkeley with lines of credit. It is axiomatic that the extension of credit is accompanied by the risk of loss.[FN56] Thus, in maintaining its processing relationship with Berkeley, each bank was subjecting itself to risk. Furthermore, there was testimony indicating that the merchant banks would have cut off their respective relationships with Berkeley if the chargeback ratio had exceeded 1%. Consequently, one may reasonably conclude that, because of the chargeback scheme, banks retained risks that they would otherwise have shed. As a result, there was sufficient evidence to suggest that the defendants acted with the requisite intent to defraud.

> FN56. **Warshak** notes that the merchant banks and the processors had created large reserves to guard against potential losses associated with chargebacks. However, there is testimony in the record indicating that the reserves might have been insufficient to mitigate the entirety of the risk.

***316** Finally, Harriet argues that the evidence proffered at trial fails to establish that she knowingly participated in the chargeback-manipulation scheme. She argues, as she did with respect to the conspiracy count, that she was merely a maternal marionette in her son's operation. She contends that she simply hit a button and had no knowledge that she was being used to manipulate the chargeback ratio. For the reasons addressed *ante* at II.F.2, this argument again falls flat.

I. Conspiracy to Commit Access-Device Fraud (18 U.S.C. § 1029)

[41] **Warshak's** next argument is that there was insufficient evidence to support his conviction for conspiracy to commit and attempt to commit access-device fraud, in violation of 18 U.S.C. § 1029(a)(5), (b)(1)-(2). Under 18 U.S.C. § 1029(a)(5), "[w]hoever ... knowingly and with intent to defraud effects transactions, with 1 or more access devices [such as credit cards] issued to another person or persons, to receive payment or any other thing of value during any 1-year period the aggregate value of which is equal to or greater than $1,000" is guilty of access-device fraud. *See United States v. Tunning*, 69 F.3d 107, 112 (6th Cir.1995) ("The definition of 'access device' includes a credit card."). An attempt to violate this statute results in "the same penalties as those prescribed for the offense attempted." 18 U.S.C. § 1029(b)(1). Additionally, those who conspire to violate the statute are subject to slightly diminished penalties. *See* 18 U.S.C. § 1029(b)(2).

Warshak was charged with a single count of conspiracy to commit and attempt to commit access-device fraud (Count 29). The indictment alleged that **Warshak** conspired to harvest customers' credit cards from Berkeley's database and charge them various amounts without the customers' consent. The indictment also alleged that this was done for the purpose of lowering Berkeley's chargeback ratio.

Admitting that "Berkeley charged customers' credit cards without authorization to reduce the chargeback ratio," **Warshak** contends that the government nonetheless failed to prove that he had the specific intent to defraud and that he conspired to obtain payment from the cards of more than $1,000. Appellant's Br. at 120. He notes that, in charging the customers, he "never intended for any of the cardholders to lose so much as a dollar." Appellant's Br. at 121. Additionally, he observes that "Berkeley's actions in debiting various customers' credit cards did not deprive the cardholders of any property or thing of value totaling more than $1000, because Berkeley on virtually every occasion immediately credited back the debit." *Ibid.*

Warshak's argument fails for a number of reasons. First, the fact that he only intended for Berkeley's customers to be temporarily parted from their money has no bearing on the issue of intent to defraud. "Whether he intended that the effects of his fraud be permanent or temporary has no legal relevance." *United States v. Olson*, 925 F.2d 1170, 1175 (9th Cir.1991), *abrogated on other grounds by United States v. Cotton*, 535 U.S. 625, 122 S.Ct. 1781, 152 L.Ed.2d 860 (2002). Thus, the testimony that **Warshak** deliberately charged customers' credit cards without permission is sufficient to establish specific intent.

[42] Similarly, it is of no consequence that Berkeley's access to the fraudulently obtained funds was ephemeral. Under the plain language of the statute, a defendant need only "receive" the requisite amount in order to violate the statute. 18 U.S.C. § 1029(a)(5). The statute does not require that the defendant "keep" or "retain" the payment. Consequent-

ly, because there *317 was testimony that 6,000 customers were charged $4.50 each in December 2003, **Warshak's** conviction was supported by competent evidence.

J. Money Laundering (18 U.S.C. §§ 1956, 1957)

1. *Promotional Money Laundering*

[43] **Warshak** argues that the government failed to present sufficient evidence that he committed various acts of so-called promotional money laundering. Promotional money laundering is defined in 18 U.S.C. § 1956(a)(1)(A)(i), which states:

> Whoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity ... with the intent to promote the carrying on of specified unlawful activity ... shall be [subject to criminal penalties].

To prove a defendant guilty of promotional money laundering, the government must demonstrate that he: "(1) conducted a financial transaction that involved the proceeds of unlawful activity; (2) knew the property involved was proceeds of unlawful activity; and (3) intended to promote that unlawful activity." *United States v. Haun*, 90 F.3d 1096, 1100 (6th Cir.1996). The paradigmatic example of this crime is a drug dealer using the proceeds of a drug transaction to purchase additional drugs and consummate future sales. *See, e.g., United States v. Torres*, 53 F.3d 1129, 1137 n. 6 (10th Cir.1995).

[44] In the present case, **Warshak** was charged with six counts of promotional money laundering (Counts 77-80, 82, 98).[FN57] Counts 77 and 78 related to million-dollar payments **Warshak** made to his sisters Sue Cossman and Cindy Hall, both of whom worked for Berkeley. Count 79 dealt with a third million-dollar payment **Warshak** made to James Doyle, another Berkeley employee and a longtime friend of **Warshak's** mother. Appellant's Br. at 128. Count 80 described a payment of $100,000 to Strong Foundations, Inc., "a purported non-profit charitable entity by which [Berkeley] would provide homes to single-parent households." Count 82 involved a transfer of $180,000 to Hallmark Homes, LLC, a Kentucky corporation owned by one of **Warshak's** brothers-in-law. Finally, Count 98 pertained to a transfer of $1 million to Harriet, **Warshak's** mother.

> FN57. **Warshak** was also charged with conspiracy to commit promotional money laundering (Count 30). However, he makes no arguments that are specific to the conspiracy charge.

Arguing that he should not have been convicted of any of these counts, **Warshak** claims that there was not enough evidence to establish the first element of the crime, namely, that the charged transactions involved the proceeds of an unlawful activity. **Warshak** renews his argument that the government failed to prove that he committed mail, wire, or bank fraud. He argues that, without the underlying convictions, there are no illegal activities from which proceeds could have been derived. He also argues that, even if his convictions were proper, the transactions at issue occurred in 2004 or later, by which time the company was "gross[ing] hundreds of millions of dollars in legitimate sales." Appellant's Br. at 126. He contends that "[t]he fact that the monies at issue originated at Berkeley ... does not, therefore, suffice to prove that the transactions at issue involved the proceeds of mail or wire fraud."[FN58] *Ibid.*

> FN58. **Warshak** also argues the government failed to prove that the proceeds were the result of bank fraud, but this issue need not be taken up; there is a plethora of evidence from which a reasonable juror could conclude that the transactions involved the proceeds of mail or wire fraud.

***318 Warshak's** argument fails. As an initial matter, a reasonable juror could easily conclude that Berkeley's sales operation was, for the entire duration of its existence, little more than a colossal fraud. *See supra* Part II.F; *see also United States v. Warshak*, 562 F.Supp.2d 986, 996 (S.D.Ohio 2008) ("The evidence showed a large and profitable consumer fraud scheme, which the jury could easily conclude resulted in proceeds the Defendants concealed or used to further the business."). Furthermore, even allowing that some of the sales were legitimate, the evidence nonetheless indicates that many of Berkeley's sales during the relevant time period were generated through deceptive practices rising to the level of mail

fraud. Because the proceeds from fraudulent sales were mixed with the proceeds of any arguably above-board sales, any transaction involving Berkeley's revenues can be said to involve the proceeds of an illegal activity. *See* *United States v. Jamieson*, 427 F.3d 394, 404 (6th Cir.2005) ("[N]ot all of the money involved in the transactions must be derived from the unlawful activity. When money from illegal sources is co-mingled with money from unspecified other sources, all such funds are attributable to the money laundering scheme." (internal citations and quotation marks omitted)).

Warshak also argues that the evidence was insufficient to establish that the transactions at issue were undertaken for the purpose of promoting a specified unlawful activity. He notes that most of the charged transactions involved gifts to family and friends. Indeed, Counts 77-78, 80, and 98 were based on checks made out to his sisters, his mother's boyfriend, and his mother, respectively. He also observes that the checks were delivered to his family members with letters that lauded their loyalty and support,[FN59] and he argues that, given his relationships with these individuals, the government failed to prove that the payments were intended to advance Berkeley's fraudulent scheme.

> FN59. Specifically, the letters stated: "Thank you for all of your help and support the last 37 years. This one is for our family, all of us. I love you."

This argument presents a fairly close question. It is true that the transactions charged in these counts were payments to Berkeley employees, and it is also true that a number of cases support the proposition that payments to employees may constitute sufficient evidence of an intent to promote an unlawful activity. *See* *United States v. Alerre*, 430 F.3d 681, 693 (4th Cir.2005) ("[T]he promotion element [was] satisfied when a defendant paid his subordinate employee for being involved in an unlawful scheme, because such payments compensated the employee for his illegal activities and encouraged his continued participation."); *see also* B. Frederic Williams, Jr. & Frank D. Whitney, Federal Money Laundering: Crimes and Forfeitures 137 (1999) ("A manufacturer of cars would think it strange if one asserted that the payment of wages for its workers on the assembly line and for steel or other raw materials were not intended to help promote the company's continuation and success in the car industry."). However, in this case, the employees to whom the payments were made had close personal relationships with **Warshak**; two of the payments went to **Warshak's** sisters, one went to his mother, and one went to his mother's close friend. The payments could therefore be seen as resulting from ***319** the magnanimity of a dutiful brother, son, and friend. Moreover, there is no direct evidence that the payments were intended as compensation for services performed on the company's behalf-*i.e.,* the payments were not listed as salary. As a result, the circumstances of the present case differ from those of a run-of-the-mill case involving direct remuneration of a mere worker.

Nonetheless, the evidence was sufficient to permit a reasonable juror to conclude that the payments were intended to promote a specified unlawful activity. The fact remains that every one of the individuals to whom a payment was made was a Berkeley employee. A juror could look at this fact and conclude that the payments were intended to reward faithful service and encourage future commitment to the criminal endeavor. Ironically, such a conclusion might actually garner support from **Warshak's** letters, in which he thanked his relatives for their "loyalty and support." Appellant's Br. at 128. Consequently, it cannot be said that the government failed to carry its evidentiary burden with respect to the million-dollar payments.

Additionally, there was sufficient evidence to permit the conclusion that the payments to Strong Foundations, Inc., and Hallmark Homes, LLC, were made with an intent to promote the fraudulent scheme.[FN60] At trial, there was testimony that Strong Foundations was a charity that funded homes for single-parent households,[FN61] and there was also testimony that Hallmark Homes, LLC, was a company that built houses. A reasonable juror could conclude that the payments to these entities were intended to raise Berkeley's philanthropic profile and create an "aura of legitimacy." *United States v. Bolden*, 325 F.3d 471, 489 (4th Cir.2003). Thus, a rational finder of fact could infer that the intent element was satisfied, and **Warshak's** challenge to the sufficiency of the evidence fails.

> FN60. The defendants make very little effort to develop this argument, stating only that

there was no evidence that the payments were intended to promote an unlawful activity. We could therefore conclude that the argument is waived. *See* *United States v. Elder*, 90 F.3d 1110, 1118 (6th Cir.1996) ("[I]t is a 'settled appellate rule that issues adverted to in a perfunctory manner, unaccompanied by some effort at developed argumentation, are deemed waived.' " (quoting *United States v. Zannino*, 895 F.2d 1, 17 (1st Cir.1990))). However, we decline to do so.

FN61. At the forfeiture phase of the trial, a defense witness testified that Strong Foundations was "a charity that Steve [**Warshak**] wanted to start in association with Berkeley to raise money through [its] customers and employees to build homes for single parent or unfortunate families in Cincinnati."

2. *Concealment Money Laundering*

[45] The defendants-here, **Warshak**, Harriet, and TCI-argue that the evidence was insufficient to establish that they committed certain acts of concealment money laundering. Like promotional money laundering, concealment money laundering is defined in 18 U.S.C. § 1956(a), which states, in relevant part:

> Whoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity ... knowing that the transaction is designed in whole or in part ... to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity ... shall be [subject to criminal penalties].

18 U.S.C. § 1956(a)(1)(B)(i). To make out a violation of this provision, the government must prove three elements: " '(1) use ***320** of funds that are proceeds of unlawful activity; (2) knowledge that the funds are proceeds of unlawful activity; and (3) ... [knowledge] that the transaction is designed in whole or in part to disguise the ... source, ownership or control of the proceeds.' " *United States v. Marshall*, 248 F.3d 525, 538 (6th Cir.2001) (quoting *Prince*, 214 F.3d at 747).

a. ***Warshak** & TCI*

[46] **Warshak** was charged with approximately sixty-five counts of concealment money laundering (Counts 32-76, 81, 83-97, 102-06).[FN62] TCI was also named in approximately twenty-one of those counts (Counts 57-58, 60-73, 79, 83, 91-93). The transactions on which the counts were based involved an assortment of business accounts, personal accounts, investments, and purchases.

FN62. **Warshak** was also charged with conspiracy to commit concealment money laundering, in violation of 18 U.S.C. § 1956(h) (Count 30). As before, he makes no arguments specific to the conspiracy count.

Warshak and TCI argue that the government failed to prove that the transactions were made with the intent "to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds." 18 U.S.C. § 1956(a)(1)(B)(i). They note that "[m]ost of the charged transactions were completely open transfers of funds to **Warshak** personally, into accounts bearing his name, or to family members with the surname **Warshak**, or to corporations of which **Warshak** was the owner and 100% shareholder and with which he was openly and publicly affiliated." Appellant's Br. at 130-31. The defendants also note that many of the charged transactions were simply transfers to and from "companies and accounts openly associated with **Warshak**." *Id.* at 131. In addition, the defendants observe that some of the "charged transactions involved purchases of investment products such as life insurance policies and annuities in **Warshak's** own name, the simple and visible spending of money that falls outside the ambit of § 1956." *Id.* at 132. In sum, the defendants contend that the transactions were all benign and transparent and that their convictions for concealment money laundering were simply not supported by the evidence.

While superficially attractive, the defendants' position overlooks several key points. It is certainly true that a number of the transactions were made under relatively open circumstances. However, that does not foreclose the possibility that the transactions were designed to conceal some characteristic of the funds involved. As this court noted in *Marshall*, "[t]he fact that a defendant personally engages in a transaction without trying to disguise his or her identity ... does not negate the effect of other evidence pointing to an intent to conceal." 248 F.3d at 539; *see* *United States*

v. Lovett, 964 F.2d 1029, 1034 (10th Cir.1992) ("Even though the defendant made no efforts to conceal his identity ... the evidence sufficiently supports the inference that a concealment occurred in another sense.").

In this case, there was other evidence that the defendants intended to conceal the exact source of the proceeds. Specifically, the government introduced the testimony of Jerry Simpson, an FBI-Special-Agent-turned-contractor whom the government had hired to investigate **Warshak's** finances. Simpson testified that "[t]he transactions [involved in the case] were very complex, some of the most complex and lengthy transactions that I have ever had the occasion to examine." Simpson also testified that "there were hundreds of deposits, withdrawals, transfers,***321** debits, credits; it was very, very complicated, very voluminous, and this is only for, you know, roughly a year and eight months of the period of the evidence." According to Simpson, the effect of the transactions, in their immense complexity, "was to conceal the commingling of business transactions and personal account transactions ... to transfer funds to Mr. **Warshak**...."

This evidence was sufficient to support a finding of intent to conceal. When a sequence of transactions is "sufficiently complex," a reasonable juror may infer that the transactions were made for the purpose of concealment. *United States v. Adefehinti*, 510 F.3d 319, 323 (D.C.Cir.2007) (quoting *United States v. Esterman*, 324 F.3d 565, 572 (7th Cir.2003)); *see United States v. Majors*, 196 F.3d 1206, 1214 (11th Cir.1999) ("Moving money through a large number of accounts ... has also been found to support the design element of money laundering...."); *United States v. Beddow*, 957 F.2d 1330, 1335 (6th Cir.1992) ("[T]he evidence of Beddow's convoluted financial dealings with his banks and his charter boat business further support a conclusion that he intended to disguise the illegal source of his money."). Here, Simpson's testimony indicated that the transactions were quite complex, and the conclusion that they were undertaken to conceal the source of the money is not unreasonable.[FN63]

FN63. **Warshak** contests this conclusion, pointing to this court's recent decision in *United States v. Faulkenberry*, 614 F.3d 573 (6th Cir.2010). There, we held that, "[t]o prove a violation of [the concealment subsection], it is not enough for the government to prove merely that a transaction had a concealing effect. Nor is it enough that the transaction was *structured* to conceal the nature of illicit funds." *Id.* at 586. However, the *Faulkenberry* court went on to acknowledge that, "depending on context, proof that a transaction was structured to conceal a listed attribute of the funds can yield an inference that concealment was a *purpose* of the transaction." *Ibid.* (emphasis added). We think that, in this case, given the complexity and numerosity of the transactions, we cannot hold that a rational juror could not infer that the transactions were undertaken with intent to conceal.

Nor is that conclusion undermined by the fact that some of the charged transactions involved the purchase of an annuity or an insurance policy. While it is true that § 1956(a)(1)(B)(i) does not criminalize the simple spending of illegally obtained money, *see United States v. Garcia-Emanuel*, 14 F.3d 1469, 1476 (10th Cir.1994) (holding that § 1956 "is a concealment statute-not a spending statute"), the purchases at issue here occurred at the end of a chain of transactions, allowing the inference that the expenditures were made with an intent to conceal as well as an intent to purchase, *see United States v. Burns*, 162 F.3d 840, 848 (5th Cir.1998) ("[A] particular transaction must be viewed in context when determining whether it was designed to conceal.").[FN64]

FN64. In *Marshall*, this court cautioned against inferring the intent behind one transaction from the intent behind the previous transaction. 248 F.3d at 540. If one could simply conclude that all transactions following an act of money laundering were made with an intent to conceal, "[a] defendant would ... be exposed to criminal liability for every derivative transaction regardless of his or her actual intent." *Ibid.*; *see also Majors*, 196 F.3d at 1212 n. 14 ("Money laundering is not a continuing offense."). However, *Marshall* dealt with a fairly simple set of facts. There, the defendant was convicted of laundering funds by (1) placing them in an investment account and (2) later spending them on several items. The *Marshall* court

> held that one could not infer an intent to conceal with respect to the purchases. The present case, by contrast, is more complex. Here, there are numerous transfers that later culminate in purchases. Given the complexity of the initial transfers, it can be reasonable to infer that the subsequent purchases were also made with an intent to conceal. Additionally, the purchases at issue in this case were often very large, which distinguishes them from the smaller purchases made in *Marshall*. *See* 248 F.3d at 531 (describing the purchase of a Rolex watch, a tennis bracelet, and wine).

***322** In addition to being convicted of the foregoing charges, **Warshak** was found guilty of concealment money laundering in connection with 49 cash shipments made to his home in San Diego, California (Count 108). Between 2002 and 2004, **Warshak** repeatedly instructed Berkeley employees to cash $5,000 checks drawn on Berkeley accounts and ship him the cash via FedEx. Sam Grote testified that he "would go to the bank, cash [the checks] for large bills, put the bills in a FED-X [sic] envelope, and send them to [**Warshak**] at his house in California." Grote also testified that he and another employee "would [sometimes] do it together."

Warshak argues that the evidence was insufficient to demonstrate that these transactions were intended to conceal the nature, source, location, ownership, or control of the funds. In making this argument, he relies on *Cuellar v. United States*, in which the Supreme Court stated: "*how* one moves the money is distinct from *why* one moves the money. Evidence of the former, standing alone, is not sufficient to prove the latter." 553 U.S. 550, 566, 128 S.Ct. 1994, 170 L.Ed.2d 942 (2008).

But the facts of this case are readily distinguishable from those confronted in *Cuellar*. There, the Supreme Court encountered a situation in which an individual was apprehended while crossing the United States-Mexico border in a Volkswagen Beetle with a secret compartment containing $81,000 in cash. *Id.* at 553-54, 128 S.Ct. 1994. Ultimately, the Supreme Court found that "[t]he evidence suggested that the secretive aspects of the transportation were employed to *facilitate* the transportation ... but not necessarily that secrecy was the *purpose* of the transportation." *Id.* at 567, 128 S.Ct. 1994.

In the present case, the facts are different. The method of transportation does not suggest that the money was only concealed for the purposes of getting it from Point A to Point B. Indeed, placing stacks of money in FedEx envelopes is not the most prudent way to keep them hidden. Furthermore, the manner in which the funds were transported is not the only relevant evidence in the record. There is also testimony that the funds were removed from Berkeley's business accounts and shipped directly to **Warshak's** personal address. That testimony suggests that the transactions themselves were designed to conceal where the money came from, not where it was at a given moment. Consequently, *Cuellar* does not mandate reversal of **Warshak's** conviction.

b. *Harriet*

[47] Harriet was also convicted of concealment money laundering, though she was only charged with four counts (Counts 99-101, 107). Harriet's convictions related to a $1 million transfer from **Warshak**. After receiving the money, Harriet placed it into an account in her name at USB Financial Services, a transaction that formed the basis for Count 99. She then removed $250,000 to open an annuity account (Count 100) and another $250,000 to place into a life insurance account (Count 101). Finally, she transferred $467,940 into an investment account, also in her name (Count 107).

Harriet argues that the government failed to prove that she knew these transactions were designed to conceal an attribute of the transferred funds. She contends that she simply received a large monetary gift from her son and then used ***323** it. She notes that the four accounts into which the money was placed all bore her name, which would cut against a finding that her purpose in making the deposits was to conceal the source of the money. She also notes that the transactions for which she was responsible were all relatively simple in nature: she took $1 million and split it into three relatively large chunks.

This argument has merit. In order for Harriet to be convicted of concealment money laundering, *she* must have had knowledge that the transactions were designed to conceal some aspect of the money at issue. It is true that the government put on evidence implicating Harriet in the conspiracy to commit mail, wire, and

bank fraud. It is also true that Harriet could be inferred to know that the $1 million gift involved the proceeds of that fraud. *See United States v. Benjamin,* 252 F.3d 1, 8 (1st Cir.2001) ("Benjamin's conviction for bank fraud provided evidence that he realized the funds originally in the Eastside Motorsports account-which were then used to obtain the bank checks-were derived from criminal activity."). However, there is no evidence that supports the conclusion that Harriet knew the gift from her son was intended to conceal the source of the funds. The government did not demonstrate, for example, that Harriet knew anything about the complex crisscross of transactions that led to the gift. Nor did the government show that **Warshak** gave any indication to his mother that the gift was being made *sub rosa.* As a consequence, no reasonable juror could properly infer that Harriet had knowledge of the intent behind the gift. We therefore reverse Harriet's conviction on Count 99.

Her convictions stemming from subsequent transfers to different accounts are also reversed. Those transfers were relatively simple and involved large amounts that would not easily have escaped the notice of banks and regulators. [FN65] Consequently, the nature of the transactions lends no circumstantial support to the notion that they were made for the purposes of concealment. *See United States v. Johnson,* 440 F.3d 1286, 1293 (11th Cir.2006) ("[A] money laundering concealment conviction pursuant to § 1956 requires evidence of something more than a simple transfer of funds between two accounts, each bearing the parties' correct name."). There was thus no competent evidence on the record supporting Harriet's convictions on Counts 100, 101, and 107. As a result, these convictions cannot stand.

> FN65. Granted, the fact that a given transfer is large or conspicuous does not preclude the finding that the transfer violated 18 U.S.C. § 1956. *See Lovett,* 964 F.2d at 1034. However, the size of the transfers is a proper consideration when determining whether the context supports a finding of intent to conceal. Here, given the relative simplicity of the transfers, the fact that large amounts were involved becomes more probative of the lack of intent.

[48] Harriet was also convicted of two counts of conspiracy to commit money laundering, in violation of 18 U.S.C. § 1956(h) (Counts 30-31). The conspiracy convictions appear to rest on the evidence offered to demonstrate that Harriet engaged in substantive money laundering. [FN66] Consequently, because the government has failed to establish that Harriet knew of the intent behind the transfer, her conspiracy convictions also fall.

> FN66. The indictment alleges that Harriet aided the conspiracy by "causing fraud proceeds to be transferred out of the accounts of [**Warshak**] and into other accounts." Presumably, this is simply a reference to the $1 million transfer.

***324** 3. *The Government's Expert Witness*

[49] The defendants argue that the district court erred by permitting the government's expert witness, Special Agent Jerry Simpson, to testify that the defendants had the mental state required to commit money laundering. [FN67] "We review 'the district court's evidentiary decisions for abuse of discretion' and should only reverse when 'such abuse of discretion has caused more than harmless error.' " *McCombs v. Meijer, Inc.,* 395 F.3d 346, 358 (6th Cir.2005) (quoting *Cooley v. Carmike Cinemas, Inc.,* 25 F.3d 1325, 1330 (6th Cir.1994)). An error is harmless "unless it is more probable than not that the error materially affected the verdict." *United States v. Martin,* 897 F.2d 1368, 1372 (6th Cir.1990).

> FN67. Because Harriet's convictions have already been found improper, this argument is relevant only to **Warshak** and TCI.

[50] Under Federal Rule of Evidence 704(b), an expert witness is not permitted to opine on the issue of "whether the defendant did or did not have the mental state or condition constituting an element of the crime charged or of a defense thereto." *See Combs,* 369 F.3d at 940 ("Rule 704(b) ... prevents an expert witness from testifying that a defendant in a criminal case did or did not have the requisite mental state or condition constituting an element of the crime charged, as ultimate issues are matters for the trier of fact.").

At trial, Agent Simpson made three statements that the defendants contend violated this rule. First, Simpson stated that "the business dealings of TCI Media were commingled with the personal dealings of Mr. **Warshak**[,] and ... it was done with *an intent to conceal* the true nature and disposition of the funds

that came in and out of the TCI Media account." Second, on cross-examination, Simpson testified that certain cash transactions "were *designed to conceal* money laundering." Finally, during redirect, Simpson stated that the defendants had made "transfers among ... various business and personal accounts that were multi-layered transactions that, in [his] opinion, were *designed to conceal* the true source and application of the funds." This testimony was allowed to stand over the defense's rather ardent objections that Simpson had violated Rule 704(b).

Notwithstanding the district court's reluctance to exclude them, Simpson's statements clearly ran afoul of Rule 704(b). In suggesting that certain transactions were undertaken with "an intent to conceal," Simpson spoke directly to the core issue of the requisite *mens rea.* That is impermissible. Furthermore, Simpson's remarks with respect to the "design" of the transactions also implicate the issue of intent. To say that a transaction is designed to achieve a certain effect is tantamount to declaring that the individual who conducted the transaction intended to achieve that outcome. *See United States v. Willey,* 57 F.3d 1374, 1389 n. 29 (5th Cir.1995) (implying that testimony regarding whether transactions were "designed to conceal" is forbidden under Rule 704(b)). True, a witness may permissibly testify that the *effect* of a transaction is to conceal, *see ibid.* (suggesting that an expert witness may properly testify that certain transactions "concealed" the source of the funds), but that is not what Simpson did when he stated that the intent of the transactions was to mask the source or nature of the funds at issue. Thus, it appears that the district court abused its discretion in admitting certain portions of Simpson's testimony.

***325** However, reversal is not appropriate in this case, as any improprieties in Simpson's testimony were harmless.[FN68] The jurors were faced with evidence of an expansive and convoluted tangle of financial transactions, evidence that would, standing alone, be more than sufficient basis to support the conclusion that **Warshak's** intent in making the charged transactions was to conceal the source of the funds. *See Garcia-Emanuel,* 14 F.3d at 1476 (holding that intent to conceal can be inferred from "a series of unusual financial moves [culminating] in the transaction"). Furthermore, although Simpson did remark that the transactions were conducted with a certain intent, the government's attorneys later clarified before the jury that they were "only asking for [his] opinion with respect to the transactions, and [that they were not] asking for [him] to make any reference or render any opinion with respect to any person's state of mind or intent[.]" Additionally, as the government notes, Simpson's final statement to the jury on direct examination was that the "*effect* [of the transactions] was to conceal." We therefore hold that reversal on the basis of Simpson's statements is inappropriate.

> FN68. Reversal of **Warshak** and TCI's convictions, that is. For the reasons discussed above, there are independent grounds to reverse Harriet's convictions.

K. Conspiracy to Obstruct an FTC Proceeding (18 U.S.C. §§ 371, 1505)

[51][52] **Warshak** argues that the government failed to prove him guilty of conspiracy to obstruct an FTC proceeding, in violation of 18 U.S.C. §§ 371 and 1505. To obtain a conviction for that offense, the government must demonstrate three elements: "(1) the existence of an agreement to violate [§ 1505]; (2) knowledge and intent to join the conspiracy; and (3) an overt act constituting actual participation in the conspiracy." *United States v. Hughes,* 505 F.3d 578, 593 (6th Cir.2007). To prove a violation of § 1505, the government must show: "(1) that there was an agency proceeding; (2) that the defendant was aware of that proceeding; and (3) that the defendant 'intentionally endeavored corruptly to influence, obstruct or impede the pending proceeding.' " *United States v. Bhagat,* 436 F.3d 1140, 1147 (9th Cir.2006) (quoting *United States v. Price,* 951 F.2d 1028, 1031 (9th Cir.1991)).[FN69]

> FN69. The government contends that the elements of the offense are somewhat different, citing *United States v. Blackwell,* 459 F.3d 739, 761-62 (6th Cir.2006). However, 18 U.S.C. § 1505 appears to set forth two separate offenses, and *Blackwell* does not pertain to the form of obstruction that is at issue in the present case.

1. *Background*

In summer 2003, the FTC began investigating Berkeley, initially focusing on the claims made in Berkeley's advertisements and later focusing on the auto-ship program. In connection with the investigation-which had the potential to result in a substantial

money judgment against both Berkeley and **Warshak**-the FTC sought certain financial information from Berkeley, eventually providing the company with a number of financial-disclosure forms in late 2004.

In summer 2004, before the forms had been sent, **Warshak** began planning his estate with the assistance of Chris Sega, a partner at an outside law firm. The planning culminated in the creation and funding of two trusts-one for **Warshak's** wife and one for his children. At **Warshak's** trial, William Bertemes, **Warshak's** accountant, testified that the timing of the estate planning was dictated by the FTC litigation. According to Bertemes, the ***326** trusts were created to remove **Warshak's** personal assets from the FTC's reach.

2. *Sufficiency of the Evidence*

Warshak argues that the evidence presented at trial was insufficient because it did not show that he intended for the creation of the trusts to impede the ongoing FTC proceeding. In support of his argument, he points to email traffic in which he suggested that "the FTC thing [would] be okay" and that he did not want to "tie up too much money in intricate trusts." He also argues that he eventually disclosed the existence of the trusts-voluntarily. Finally, he argues that the creation of the trusts was motivated in large part by the advice of his lawyers, who urged him "to divide his assets with his spouse for estate planning purposes." Appellant's Br. at 146.

Though the evidence in this case is extremely close, given the stringency of the standard set forth in *Jackson*, we affirm **Warshak's** conviction. While there is certainly language in **Warshak's** emails indicating that he may not have been motivated by a desire to obstruct the FTC investigation, there is also competent evidence in the record that his decision to create and fund the trusts was, at least at one point, motivated by the desire to shield his assets from the FTC. Bertemes testified that the creation of the funds was justified as an estate-planning measure but was in fact undertaken for "litigation" purposes. In addition, though **Warshak** was initially hesitant to place money in the trusts, he eventually endowed them with over $14 million, money that his emails indicate he was extremely reluctant to part with. Notably, the transfers took place just one week after the FTC sent financial disclosure forms to Berkeley. Although **Warshak** did eventually disclose the existence of the trusts, that does not mean that he was always intent on doing so. Furthermore, when disclosure was finally made, more than seven months later, the assets had already been frozen in connection with the government's criminal investigation into Berkeley's operations.[FN70] Thus, based on the evidence available at trial, a reasonable juror could conclude that **Warshak** entered into an agreement to impede the FTC proceeding.[FN71]

FN70. The **Warshak** family accounts were all frozen pursuant to seizure warrants.

FN71. **Warshak** argues that he should not have been convicted because his actions did not have the "natural and probable effect" of undermining the FTC proceeding. In making this argument, he points to the Supreme Court's decision in *United States v. Aguilar*, 515 U.S. 593, 599, 115 S.Ct. 2357, 132 L.Ed.2d 520 (1995). There, the Court noted that, "if the defendant lacks knowledge that his actions are likely to affect the judicial proceeding, he lacks the ... intent to obstruct [required under 18 U.S.C. § 1503]." *Ibid.* But *Aguilar* involved obstruction of a judicial proceeding, not obstruction of an agency proceeding. Thus, we find *Aguilar* inapposite. *See Bhagat*, 436 F.3d at 1147-48 (declining to read an additional element into § 1505 on the basis of the Supreme Court's decision in *Aguilar*).

L. Disclosure of Searches & Seizures

[53] Before trial, the defendants filed a motion asking that the district court "order the government to affirm or deny whether any interceptions, searches, seizures, orders, or subpoenas of their communications ha[d] occurred." The district court denied the motion, explaining that Federal Rule of Criminal Procedure 16 only requires the government to disclose certain types of evidence. The district court also noted that the government had indicated it would "turn over at the appropriate***327** time any Jencks Act or *Brady* materials."

The defendants now argue that the district court erred in denying their motion. They claim that "Rule 16 provide[s] a floor, but not a ceiling, on the government's disclosure obligations...." Appellant's Br. at 148. In addition, they argue that, without disclosure of

the government's investigative practices, they would have no way of knowing whether their Fourth Amendment rights were being trampled. Invoking the government's "almost limitless technological capacity to secretly search computers and electronic communications," the defendants essentially argue that discovery should serve as another check on the government's electronic incursions into the privacy of citizens.

But the defendants cite no authority in support of their position. There is, however, authority for the proposition that the government's discovery obligations are limited. In *United States v. Presser,* this court held that "Rule 16 requires the government to disclose to the defense before trial only specific categories of evidence." 844 F.2d 1275, 1284 (6th Cir.1988). Those categories include:

> prior statements of the defendant, the defendant's prior criminal record, documents, photographs, or tangible objects, which are within the custody or control of the government and which are material to the defense or intended for use by the government in its case-in-chief at trial or which were obtained from or belong to the defendant, and the results of any mental or physical examinations performed on the defendant which are material to the defense or which are intended for use by the government as evidence in its case-in-chief at trial.

Id. at 1284-85. Furthermore, the *Presser* court held that "the discovery afforded by Rule 16 is limited to the evidence referred to in its express provisions." *Id.* at 1285. Consequently, "[t]he rule provides no authority for compelling the pre-trial disclosure of *Brady* material, or of any other evidence not specifically mentioned by the rule." *Ibid.* (internal citations omitted). In light of this precedent, we hold that the district court did not abuse its discretion in denying the defendants' discovery motion. *See Gray,* 521 F.3d at 529 (holding that a district court's discovery rulings are reviewed for abuse of discretion).

M. Sentencing Issues

1. *Background*

The defendants were sentenced on August 27, 2008. Prior to their individual hearings, the district court summoned all of the defendants and explained the amount of loss that it would use for purposes of determining the applicable offense level under USSG § 2B1.1(b). The district court's explanation went as follows:

> [The] [d]efendants essentially attempt[ ] to minimize their conduct based on the relative number of complaints to their overall sales based on the number of refunds made. Yet, their assertions are belied by the tens of thousands of claimants in the consumer class action against Berkeley settled in a Montgomery County Common Pleas Court and by Berkeley's settlement by the Attorneys General for Ohio, Arkansas, Florida, Missouri, North Carolina, Oregon, Pennsylvania, Virginia, Washington, Wisconsin and the District of Columbia. This was a series of massive fraud schemes that affected thousands of individuals.
>
> The Court recognizes the difficulty in determining the amount of loss suffered by the victims of the defendants' various fraudulent activities.
>
> Since the amount of loss reasonably cannot be determined, the Court will ***328** look rather to the amount of gain resulting from such fraudulent activity. The government contends such gain amounts to in excess of $411 million dollars, which represents the net sales, being the gross sales less returns, allowances and refunds during the period of the conspiracies.
>
> The cooperating defendants, however, admitted they defrauded consumers of over $100 million dollars. Such admission of wrongful gain do[es] not cover the entire time span of the conspiracies.
>
> The defendants who were tried claim the amount of loss cannot be accurately determined, nor have they assisted the Court in determining the amount of loss the victims suffered. The Court agrees that it would be speculative to estimate the amount of loss in light of the number of claims that have been filed against Berkeley.
>
> Thus, under the advisory notes, the Court may look to gain in arriving at the appropriate figure for sentencing purposes. *To be conservative, the Court will accept the $100 million figure as the appropriate figure amounting to gain for sentencing purposes, based on the admissions of cooperating*

witnesses.

The Court further finds that restitution to the victims of defendants' conduct [is] impractical because it's too difficult to identify the victims and speculative to determine how much loss each victim actually suffered.

Appellant's App'x at 108-10 (emphasis added).

Thereafter, the defendants were sentenced individually. At **Warshak's** sentencing hearing, the district court inexplicably abandoned its original loss determination, declaring that **Warshak** would be held responsible for $411 million in losses. The district court offered no justification for deviating from its previous determination that the amount of loss would be set at $100 million. The district court then determined **Warshak's** Guidelines range to be life imprisonment, based on a total offense level of 49 and a Criminal History Category of I.

Harriet was sentenced the same day. Like **Warshak**, Harriet was held accountable for more than $400 million in losses. The district court determined that her advisory Guidelines range was also life imprisonment. Ultimately, Harriet received a sentence of 24 months.

2. *Amount of Loss*

[54] The defendants argue that the district court erred in determining the amount of loss under USSG § 2B1.1(b)(1)(P). We review a district court's determination of the amount of loss attributable to a defendant for clear error. *United States v. Jordan*, 544 F.3d 656, 671 (6th Cir.2008) (citing *United States v. Tudeme*, 457 F.3d 577, 581 (6th Cir.2006)). By contrast, we review the district court's methodology for calculating loss *de novo*. *United States v. Erpenbeck*, 532 F.3d 423, 433 (6th Cir.2008) (citing *United States v. Rothwell*, 387 F.3d 579, 582 (6th Cir.2004)). An error with respect to the loss calculation is a procedural infirmity that typically requires remand. *See Gall v. United States*, 552 U.S. 38, 51, 128 S.Ct. 586, 169 L.Ed.2d 445 (2007) (holding that improperly calculating the Guidelines range is a serious procedural error).

In *United States v. Triana*, this court provided an overview of how loss should be calculated for purposes of determining a defendant's adjusted offense level. As we explained,

> U.S.S.G. § 2B1.1 is the Guideline used by courts in determining "loss" for fraud cases. The Guideline enhances a defendant's*329 sentence to correlate to the amount of loss caused by his fraud. *See* U.S.S.G. § 2B1.1(b)(1). Application Note 2 to § 2B1.1 provides guidance for the determination of loss. The application note states that "loss is the greater of actual loss or intended loss." *Id.* § 2B1.1, cmt. (n.2) (2002). "[A]ctual loss" is "the reasonably foreseeable pecuniary harm that resulted from the offense," and "intended loss" is "the pecuniary harm that was intended to result from the offense" and "includes intended pecuniary harm that would have been impossible or unlikely to occur." *Id.* § 2B1.1, cmt. (n.2(A)(i) and (ii)). In situations where the losses occasioned by financial frauds are not easy to quantify, the district court need only make a reasonable estimate of the loss, given the available information. *Id.* § 2B1.1, cmt. (n.2(C)). Such estimates "need not be determined with precision." *United States v. Miller*, 316 F.3d 495, 503 (4th Cir.2003).
>
> 468 F.3d 308, 319-20 (6th Cir.2006) (footnotes omitted). It should also be noted that, in cases where the amount of loss cannot reasonably be determined, the court shall instead use the gain that resulted from the offense when determining the applicable enhancement. USSG § 2B1.1, cmt. n. 3(B) ("The court shall use the gain that resulted from the offense as an alternative measure of loss only if there is a loss but it reasonably cannot be determined."); *see United States v. Parrish*, 84 F.3d 816, 819 (6th Cir.1996) (employing gain as a proxy for loss in the context of § 2F1.1).

The defendants now argue that the district court's loss determination was erroneous for four reasons. First, they contend that "because loss could have been reasonably calculated, it was error to substitute [the] defendants' gain [.]" Appellant's Br. at 155. Second, they assert that "even if it were permissible to look to [the] defendants' gain as the proxy for loss, the finding that all of Berkeley's revenues were fraudulently derived was manifestly contrary to the evidence[.]" *Ibid.* Third, they argue that "the court erroneously placed the burden on [them] to prove that Berkeley revenues were not fraudulently derived[.]" *Id.* at 155-56. And fourth, they contend that the district court "did not adequately explain the rationale for its loss/gain cal-

culation." *Id.* at 156.

[55] Ultimately, we think it best to remand in this case because the district court's explanation of its loss determination was inadequate. As the defendants note, the district court did little to explain how it arrived at $411 million as the amount of loss, other than to suggest that the figure represented Berkeley's net sales. Further complicating matters is the fact that the district court originally stated that it would place the amount of gain at $100 million. Because the amount of loss was a contested issue, the district court should have engaged in a more thorough explication of its calculation, and it also should have explicitly referenced the evidence upon which it relied. *See* Fed.R.Crim.P. 32(i)(3)(B); *United States v. White*, 492 F.3d 380, 415 (6th Cir.2007). On remand, the district court should explain why it silently renounced its decision to hold the defendants responsible for only $100 million in losses.

Furthermore, we note that it may be improper to conclude that all of Berkeley's revenues constitute *actual* loss for purposes of § 2B1.1(b)(1). True, the evidence suggests that Berkeley's operations-even in the later years-were permeated with fraud, but there is no evidence suggesting that literally every customer was deceived by Berkeley's misrepresentations. In addition, there is evidence in the record that ***330** at least $25 million in sales were conducted at retail outlets. This evidence appears to indicate that some of Berkeley's sales did not actually correspond to fraudulent losses. [FN72] Of course, a district court may rely on *intended* loss when determining the amount of loss under the Guidelines, but the question of intended loss is one we leave to the district court.

> FN72. The defendants also point to evidence that "[a]pproximately 700,000 customers purchased products with no continuity program." Reply Br. at 78.

3. *Substantive Reasonableness*

Warshak also contends that his 25-year sentence was substantively unreasonable. However, because the district court erred with respect to the loss calculation, we need not reach this argument. *See* Gall, 552 U.S. at 51, 128 S.Ct. 586 (noting that review for substantive reasonableness is necessary only if the district court's decision is procedurally sound).

N. Forfeiture Issues

1. *Background*

On February 25, 2008, the trial proceeded to the forfeiture phase, during which the jury was asked to determine whether the government had established the requisite nexus between certain assets enumerated in the indictment-including homes, cars, and bank accounts-and the offenses committed by the defendants. [FN73] The forfeiture phase lasted two days, after which the jury found that the requisite nexus existed with respect to all 33 of the assets in question.

> FN73. Under Federal Rule of Criminal Procedure 32.2(b)(5)(B), "[i]f a party timely requests to have the jury determine forfeiture, the government must submit a proposed Special Verdict Form listing each property subject to forfeiture and asking the jury to determine whether the government has established the requisite nexus between the property and the offense committed by the defendant."

On May 14, 2008, the district court conducted a hearing, at which it determined the extent of the forfeiture. Thereafter, the district court held "the [d]efendants involved in the mail, wire, and bank fraud conspiracy ... jointly and severally liable for $459,540,000.00 in a proceeds money judgment and [d]efendants Steven **Warshak**, Harriet **Warshak**, and Paul Kellogg ... jointly and severally liable for $44,876,781.68 in a money laundering judgment."

2. *Exclusion of Evidence*

[56] The defendants argue that the district court erroneously excluded certain evidence from both the forfeiture phase of the trial and the subsequent hearing to determine the amount of forfeiture. We review district court evidentiary rulings for abuse of discretion. *United States v. White*, 563 F.3d 184, 191 (6th Cir.2009). "Broad discretion is given to district courts in determinations of admissibility based on considerations of relevance and prejudice, and those decisions will not be lightly overruled." *United States v. Jackson-Randolph*, 282 F.3d 369, 376 (6th Cir.2002) (citing *United States v. Hawkins*, 969 F.2d 169, 174 (6th Cir.1992)). "If we find an abuse of discretion, we [will] reverse the district court's judgment only if the error was not harmless." *Ibid.* (citing *United States v.*

Carter, 969 F.2d 197, 201 (6th Cir.1992)).

During the forfeiture trial, the defendants attempted to introduce certain evidence, which they contended would demonstrate that, from late 2003 onward, a substantial number of Berkeley's sales were legitimate.[FN74] That evidence included: ***331** notebooks of marketing materials and boxes of positive customer testimonials; examples of compliance, training, and chargeback-reduction plans; and the results of a statistical study of Berkeley's sales calls, which purportedly revealed that after 2004 disclosure was made in the vast majority of cases. When this evidence was offered, the government objected, arguing that the defendants were simply trying to relitigate the issue of guilt. The defense countered with the argument that the legitimacy of Berkeley's sales was highly relevant to the issue of nexus. After hearing the arguments, the district court sided with the government, ruling that the evidence was irrelevant.

> FN74. Before the subsequent forfeiture hearing, at which the district court determined the amount of forfeiture, the defendants again tried to introduce testimony relating to disclosure of the auto-ship program during sales calls. The district court excluded the evidence. Because the defendants do not develop their argument with respect to this evidence, it is waived. *See Slater v. Potter*, 28 Fed.Appx. 512, 513 (6th Cir.2002). In any event, even if the argument were in play, we would find it unpersuasive in light of the considerations addressed below.

Ultimately, the district court's analysis on the issue of relevance appears to be sound. As the district court noted, the jury, in reaching its verdict in the guilt phase, determined that the defendants had engaged in certain illegal conduct. The remaining question was whether *that* illegal conduct had a link to the assets listed in the indictment. Thus, the defendants' attempts to show that certain sales were not the result of illegal conduct was tantamount to reopening this issue of guilt; the defendants were seeking to show that certain acts were not unlawful, which was no longer a live issue. As a result, the district court's decision to exclude the evidence was not abuse of discretion.

3. *Sufficiency of the Evidence*

[57] The defendants also argue that there was insufficient evidence to support the forfeiture judgments. In reviewing this claim, we are mindful that "[t]he Government must prove forfeiture by a preponderance of the evidence." *United States v. Jones*, 502 F.3d 388, 391 (6th Cir.2007) (citing *United States v. Hall*, 411 F.3d 651, 654-55 (6th Cir.2005)). "[T]he district court's findings of fact are reviewed under a clearly erroneous standard and the question of whether those facts are sufficient to constitute a proper criminal forfeiture is reviewed *de novo*." *United States v. O'Dell*, 247 F.3d 655, 679 (6th Cir.2001). The district court's interpretation of the forfeiture laws is also reviewed *de novo*. *Ibid.*

a. *Proceeds Forfeiture*

The defendants argue that the government failed to prove by a preponderance of the evidence that the entirety of Berkeley's revenues-$459,540,000-constituted the proceeds of fraud. In making this argument, the defendants point, again, to the "massive ameliorative efforts directed at bringing [Berkeley's] marketing practices into full legal and regulatory compliance." Appellant's Br. at 177 n. 70. Essentially, the defendants argue that, from late 2003 onward, Berkeley was a legitimate operation, untainted by any potential fraud that may have characterized its early history. The defendants also note that approximately $25 million in sales occurred at retail outlets, such as Wal-Mart and GNC. These sales, the defendants contend, were surely legitimate, as were sales of many other products. Finally, the defendants contend that the bank-fraud scheme could not have supported a finding that all of Berkeley's proceeds were the result of unlawful activities, as the conduct alleged in the bank-fraud counts ended in January 2004. Appellant's Br. at 178. At bottom, the defendants fault the district ***332** court for simply accepting the government's assertion that everything was attributable to fraud.

[58] To demonstrate that certain property is subject to forfeiture under 18 U.S.C. § 982(a)(2), the government must show that the property constituted, or was derived from, "proceeds the [defendant] obtained directly or indirectly, as the result of [certain illegal conduct or a conspiracy to commit certain illegal conduct]." Similarly, under 18 U.S.C. § 981(a)(1)(C), the government must show that the property "constitutes or is derived from proceeds traceable to [certain illegal conduct or a conspiracy to commit certain illegal conduct]." [FN75] Notably, both

statutes require forfeiture of proceeds that result from conspiracies.

> FN75. For purposes of 18 U.S.C. § 981, "the term 'proceeds' means property of any kind obtained directly or indirectly, as the result of the commission of the offense giving rise to forfeiture, and any property traceable thereto, and is not limited to the net gain or profit realized from the offense." *Id.* § 981(a)(2)(A).

[59][60] In this case, there is sufficient evidence to conclude that the entirety of Berkeley's revenues are proceeds that resulted, whether directly or indirectly, from unlawful activity. First, as has been previously discussed, there is copious evidence indicating that Berkeley executives concocted false advertisements, concealed the existence of Berkeley's auto-ship program, limited refunds, and fed false information to its merchant banks. While the defendants contend that Berkeley's business practices were reformed in 2004, there is also evidence that things remained largely the same. For example, numerous executives testified that any "massive ameliorative efforts" were simply cosmetic changes instituted to keep the auto-ship program from getting shut down. According to various Berkeley insiders, though the existence of the auto-ship program was eventually disclosed during sales calls, the disclosures were meant to be ineffective. Furthermore, there is evidence that disclosure of the auto-ship program on the company's websites was erratic, and there is also evidence that, when it was present, the online disclosure language was confusing and deceptive. Thus, it can be concluded that, even after the company attempted to affect an air of legitimacy, the very nucleus of its business model remained rotten and malignant.[FN76] In the words of the district court, there is evidence "that the entire operation was permeated with fraud."

> FN76. The enduring nature of the corruption can also be inferred from a number of 2005 emails that **Warshak** sent to Shelley Kinmon. In one, **Warshak** pitched a new claim that "[E]nzyte is a powerful blood flow stimulator for peak circulation and fuller, larger erections-up to 25% larger according to an independent customer study." In another, **Warshak** implored Kinmon and the sales staff to emulate the creative process that led to Samuel Taylor Coleridge's "Kubla Khan." To wit, **Warshak** suggested: "THROW A SALES COPY PARTY-GET 3-4 BOTTLES OF WINE, A LARGE BONG, AND AN [8]-BALL-THEN SIT AROUND AND MAKE SHIT UP!!-THAT'S WHAT I DO.... BUT WRITE IT ALL DOWN OR YOU'LL FORGET IT THE NEXT DAY."

Moreover, the argument that certain sales were legitimate gains no traction. Any money generated through these potentially legitimate sales is nonetheless subject to forfeiture, as the sales all resulted "directly or indirectly" from a conspiracy to commit fraud. *See* 18 U.S.C. § 982(a)(2). The same can be said for any sales that occurred at retail because those sales were the outgrowth of Berkeley's fraudulent beginnings. Furthermore, it could be argued that any sales post-dating the bank-fraud counts were proceeds resulting*333 indirectly from fraud, as Berkeley would have been unable to conduct credit-card transactions if the chargeback-manipulation scheme had never been implemented. As a consequence, forfeiture of Berkeley's revenues, including money generated through supposedly legitimate transactions, was appropriate.

b. *Money Laundering Forfeiture*

The defendants also assert that the evidence was inadequate to support the money-laundering forfeiture judgment. In making this assertion, they again allege a "complete lack of evidence of any fraudulent conduct by **Warshak** or anyone at Berkeley after 2003." Appellant's Br. at 179. For the reasons discussed above, this argument gains no traction; abundant evidence indicates that the scheme persisted after the so-called "ameliorative efforts."

However, because Harriet's convictions on the money-laundering counts were improper, the evidence is necessarily insufficient to support a money-laundering forfeiture judgment against her. **Warshak**, though, remains jointly and severally liable for the entire $44,876,781.68 money laundering judgment.

III. CONCLUSION

For the foregoing reasons, we **AFFIRM** Steven **Warshak's** convictions. We also **AFFIRM** the forfeiture judgments against him, but we **VACATE** his 25-year sentence and **REMAND** for resentencing. We also **AFFIRM** TCI's convictions. In addition, we

AFFIRM Harriet **Warshak's** convictions for conspiracy to commit mail, wire, and bank fraud (Count 1); and bank fraud (Count 27). However, we **REVERSE** her convictions for conspiracy to commit money laundering (Counts 30-31) and money laundering (Counts 99-101, 107), and we **VACATE** her sentence and **REMAND.** Lastly, we **AFFIRM** the proceeds-money forfeiture judgement against her, but we **REVERSE** the money-laundering forfeiture judgment against her.

KEITH, Circuit Judge, concurring.

Although I concur in the result the majority reaches, I write separately to provide clarification concerning whether **Warshak's** emails, obtained in violation of the Fourth Amendment, should have been excluded from trial under the exclusionary rule.

I.

The Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" without warrants issued based upon probable cause. U.S. CONST. amend. IV. The exclusionary rule is a "remedy designed to safeguard Fourth Amendment rights generally through its deterrent effect...." *United States v. Leon*, 468 U.S. 897, 906, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984) (citing *United States v. Calandra*, 414 U.S. 338, 348, 94 S.Ct. 613, 38 L.Ed.2d 561 (1974)). Where evidence is collected in violation of an individual's reasonable expectation of privacy, it is subject to the exclusionary rule and will generally be suppressed at trial to deter further police misconduct in the future. *Illinois v. Krull*, 480 U.S. 340, 348, 107 S.Ct. 1160, 94 L.Ed.2d 364 (1987) (citing *Leon*, 468 U.S. at 916, 104 S.Ct. 3405). However, where an officer acts in objectively reasonable reliance upon a statute that is later found unconstitutional, exclusion of the evidence would not deter future police misconduct. *Id.* at 349, 107 S.Ct. 1160. "Penalizing the officer for the legislature's error, rather than his own, cannot logically contribute to the deterrence of Fourth Amendment violations." *Krull*, 480 U.S. at 350, 107 S.Ct. 1160 (alteration in original) (citation omitted).***334** Rather, "the greatest deterrent to the enactment of unconstitutional statutes by a legislature is the power of the courts to invalidate such statutes." *Id.* at 352, 107 S.Ct. 1160. Therefore, where an officer acts in good faith upon a statute later found unconstitutional, the evidence remains admissible in trial. *Id.* at 352-53, 107 S.Ct. 1160; *see also U.S. v. Master*, 614 F.3d 236, 243 (2010) (noting that the Supreme Court's recent jurisprudence "weighed more toward preserving evidence for use in obtaining convictions, even if illegally seized, than toward excluding evidence in order to deter police misconduct unless the officers engaged in 'deliberate, reckless, or grossly negligent conduct.' " (internal citation omitted)).

Here, we are presented with a unique situation. As the majority notes, because the government requested a secret subpoena to confiscate **Warshak's** personal emails without his knowledge pursuant to § 2703(b) and (d) of the Stored Communications Act ("SCA"),[FN1] there is no need to exclude the evidence. The officers took these actions in good faith reliance upon these statutes. They requested the emails from NuVox via a § 2703(b) subpoena and a § 2703(d) order. Though the government failed to give notice within ninety days after the initial request, it did so only after the emails had been obtained and after an initial showing that notice should be delayed. While we today declare these statutes unconstitutional insofar as they permit the government to obtain such emails without a warrant, it does not follow that the evidence should have been excluded from **Warshak's** trial. Such an exclusion would not have a substantial deterrent effect on future Fourth Amendment violations enacted by the legislature. *See Herring v. United States*, 555 U.S. 135, 129 S.Ct. 695, 700, 172 L.Ed.2d 496 (2009) (focusing on "the efficacy of the rule in deterring Fourth Amendment violations in the future"). Therefore, the majority rightfully affirms the district court's refusal to suppress **Warshak's** emails. With this I agree.

> FN1. The SCA refers generally to Chapter 121 of Title 18 of the United States Code, including sections 2701 through 2712. It was enacted as part of the Electronic Communications Privacy Act of 1986, Pub.L. No. 99-508, 100 Stat. 1848 (1986).

However, there is a further wrongdoing that troubles me today. Specifically, the government's request that NuVox preserve **Warshak's** stored and future email communications without **Warshak's** knowledge and without a warrant pursuant to § 2703(f). Under § 2703(f), "[a] provider of wire or electronic communication services or a remote computing service, upon the request of a governmental

entity, shall take all necessary steps to *preserve* records and other evidence *in its possession* pending the issuance of a court order or other process." 18 U.S.C. § 2703(f) (emphasis added). This subsection was added to the SCA in 1996 in an effort to supplement law enforcement resources and security. The Antiterrorism Act of 1996, Pub.L. 104-132, 110 Stat. 1305. While added in a completely different context from the creation of the statute, it is worthwhile to review the purpose of the statute as a whole when considering the meaning of this subsection.

Section 2703, as part of the Electronic Communications Privacy Act ("ECPA"), was enacted in 1986 as part of Congress's effort to maintain "a fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies." S. Rep. 99-541, at 4, 1986 U.S.C.C.A.N. 3555, 3559. Moreover, the advent of the ECPA was precipitated by concerns about advancements in technology and the desire to protect personal***335** and business information which individuals can no longer "lock away" with ease. The plain language of § 2703(f) permits only the preservation of emails in the service provider's possession at the time of the request, not the preservation of future emails.[FN2] Moreover, the Department of Justice, along with some theorists, emphasize that these requests "have no prospective effect." *See, e.g.,* Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act,* 72 Geo. Wash. L.Rev. 1557, 1565 (2004); U.S. Dep't of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Chapter III, § G(1) (2009), *available at* http:// www. cybercrime. gov/ ssmanual/ 03 ssma. html ("[Section] 2703(f) letters should not be used prospectively to order providers to preserve records not yet created. If agents want providers to record information about future electronic communications, they should comply with the [Wiretap Act and the Pen/Trap statute]."). I find this statutory interpretation persuasive.

> FN2. This plain reading of the statute differs from that expressed in the majority opinion. *See supra* fn. 21. Though lower courts have followed my understanding of the statute, analysis of this statute appears to be one of first impression before a circuit court. *See In re Application for Pen Register and Trap/Trace Device,* 396 F.Supp.2d 747, 760 (S.D.Tex.2005), *abrogated by In re United States for Historical Cell Site Data,* ---S.W.3d ---- (S.D.Tex.2010) (noting that the SCA is retrospective in nature as opposed to the Wiretap Act); *In re Application for U.S. for an Order Authorizing Disclosure of Location Based Services,* 2007 WL 2086663, *1 (S.D.Tex. July 6, 2007) (noting that nothing in § 2703 authorizes the Government to demand that a provider prospectively "create records which would not otherwise exist in the ordinary course of business"); *In re Application of the U.S. for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device,* 396 F.Supp.2d 294, 313-14 (E.D.N.Y.2005) (concluding, based upon the language of § 2703 as a whole, that the statute "does *not* authorize a court to enter a prospective order to turn over data as it is captured" because of the retrospective nature of the statute).

Following NuVox's policy, the provider would have destroyed **Warshak's** old emails but for the government's request that they maintain all current and prospective emails for almost a year without **Warshak's** knowledge. In practice, the government used the statute as a means to monitor **Warshak** after the investigation started without his knowledge and without a warrant. Such a practice is no more than back-door wiretapping. I doubt that such actions, if contested directly in court, would withstand the muster of the Fourth Amendment. Email, much like telephone, provides individuals with a means to communicate in private. *See* ***Warshak*** *v. United States,* 490 F.3d 455, 469-70 (6th Cir.2007), *vacated,* 532 F.3d 521 (6th Cir.2008) (en banc). The government cannot use email collection as a means to monitor citizens without a warrant anymore than they can tap a telephone line to monitor citizens without a warrant. The purpose of § 2703, along with the Stored Communications Act as a whole, is to maintain the boundaries between a citizen's reasonable expectation of privacy and crime prevention in light of quickly advancing technology. S. Rep. 99-541, at 4, 1986 U.S.C.C.A.N. 3555, 3559. To interpret § 2703(f) as having both a retroactive and prospective effect would be contrary to the purpose of the statute as a whole.

While it was not the issue in today's decision, a

policy whereby the government requests emails prospectively without a warrant deeply concerns me. I am furthermore troubled by the majority's willingness to disregard the current reading of § 2703(f) without concern for future analysis of this statute. Nevertheless, because ***336** the government's violation of the Fourth Amendment stems from the order and/or subpoena to obtain **Warshak's** email communications pursuant to § 2703(b) and (d), the government acted in good faith upon the statute. The fact that their policy likely exceeded the parameters of § 2703(f) is irrelevant to this analysis as they did not rely upon § 2703 as a whole in requesting the secret subpoena and order to obtain these emails. Accordingly, the majority was correct in holding that the evidence falls within the good faith exception to the exclusionary rule.

II.

Having addressed these matters, I **CONCUR** in the majority's decision.

C.A.6 (Ohio),2010.
U.S. v. Warshak
631 F.3d 266

END OF DOCUMENT