CRIMINAL INVESTIGATIONS AND TECHNOLOGY: PROTECTING DATA AND RIGHTS

JUNE 8, 2017

Bracewell LLP makes this information available for educational purposes.
This information does not offer specific legal advice or create an attorney-client relationship with the firm.
Do not use this information as a substitute for specific legal advice. Proprietary. Not for duplication.

Philip J. Bezanson & Shannon B. Wolf

BRACEWELL

FORMER ASSISTANT ATTY. GENERAL LESLIE R. CALDWELL

- "Innovation in computing, the Internet, and related services has had tremendous benefits for our economy . . . It has also transformed how we in law enforcement do our jobs by expanding our ability to detect, investigate and prosecute criminal activity."

- "There is nothing wrong with companies pursuing profits and marketing strategies, but . . . Our ability to protect Americans from crime has become dependent, in thousands of cases, on the business decisions of for-profit corporations. More troublingly, even when companies have the technical ability to reasonably assist us in accessing encrypted information, they have refused to do so for fear of 'tarnishing' their image."

INTRODUCTION

- As innovation continues to outpace legal and legislative developments, companies that store personal data have been in tension with law enforcement over investigation techniques.

- Law enforcement utilizes traditional criminal investigation techniques including the use of grand jury subpoenas and search warrants to obtain data and other materials from technology companies.

- The technology sector, has countered with objections under the Stored Communications Act as well as the First and Fourth Amendments to the Constitution to protect customer data and privacy.

CRIMINAL INVESTIGATIONS AND TECHNOLOGY: PROTECTING DATA AND RIGHTS

- Warrant Proof Encryption
  - Lavabit, Inc.
  - Apple Inc.
- Foreign Reach of Search Warrants
  - Google, Inc.
- Virtual Currency & the Internal Revenue Service
  - Coinbase, Inc.
- Agency Subpoenas
  - Twitter, Inc.
- Emerging Issues with New Technologies

WARRANT PROOF ENCRYPTION

RESPONDING TO A SUBPOENA AND SECRET SEARCH WARRANT WHEN CUSTOMER PRIVACY IS CRITICAL TO YOUR BUSINESS.

BRACEWELL

NEWS

DOJ says Lavabit cannot prevent search warrants by 'locking its front gate'

By John Ribeiro

Bangalore Correspondent, IDG News Service

NOV 13, 2013 9:05 AM PT

Lavabit founder refused FBI order to hand over email encryption keys

Unsealed documents show Ladar Levison, now subject of government gag order, refused requests to 'defeat its own system'

BRACEWELL

THE 18 U.S.C. § 2703 ORDERS

- Section 2703(d) permits:
  - a court order for disclosure of contents of electronic communications or records concerning electronic communication if 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.
- Section 2705(b) permits:
  - a gag order precluding the disclosure of the subpoena or warrant if notification of the existence of the warrant, subpoena, or court order will result in:
    - (1) endangering the life or physical safety of an individual;
    - (2) flight from prosecution;
    - (3) destruction of or tampering with evidence;
    - (4) intimidation of potential witnesses; or
    - (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT ("CALEA") 47 U.S.C. § 1001

- Requires companies to assist the government with the decryption of data when the company has a decryption key; does not require the company to create a decryption key.

- Does not authorize any law enforcement agency or officer to require any specific design of equipment, facilities, services, features, or system configurations to be adopted by any provider of a wire or electronic communication service, any manufacturer of telecommunications.

PEN REGISTER ACT: 18 U.S.C. § 3121

- Pen Trap Orders can require providers assist law enforcement in the installation of the trap and trace device.

- Pen Trap Orders also frequently filed under seal and prohibit providers from disclosing to the target the fact of the Pen Trap Order and data collection.

National Security

Apple vows to resist FBI demand to crack iPhone linked to San Bernardino attacks

U.S. Drops Apple Case After Getting Into Terrorist's iPhone

by **Edvard Pettersson**, **Alex Webb**, and **Chris Strohm**

March 28, 2016 5:54 PM *Updated on* March 29, 2016 12:07 PM

THE ALL WRITS ACT: 28 U.S.C. § 1651

- The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law.

- "The All Writs Act is a residual source of authority to issue writs that are not otherwise covered by statute." *Pennsylvania Bureau of Correction v. U.S. Marshals Service,* 474 U.S. 34, 43 (1985).

- Empowers courts to issue supplemental orders in furtherance of search warrants. *U.S. v. New York Telephone Co.,* 434 U.S. 159, 174 (1977)

THE ORDER COMPELLING APPLE TO ASSIST AGENTS IN ITS SEARCH:

- Required Apple to assist the FBI by providing the FBI an opportunity to determine the passcode of the iPhone; and

- Instructed Apple to provide “reasonable technical assistance” which included creating custom software that would:
  - bypass or disable the iPhone’s auto-erase function;
  - enable the FBI to submit passcodes for testing; and
  - remove any time delays between entering incorrect passcodes.

APPLE'S RESPONSE: MOTION TO VACATE ORDER

- Cautioned against the reach of the All Writs Act to compel a private company to develop software: "what is to stop the government from demanding that Apple write code to turn on a microphone in aid of government surveillance, activate the video camera, surreptitiously record conversations, or turn on the location services to track the phone's user?" *In Matter of the Search of an Apple Iphone*, 16-cm-00010 (C.D.C.A. Feb. 25, 2016) (Apple Inc.'s Motion to Vacate) at p. 4.

REMARKS OF ASSISTANT A.G. CALDWELL

- “[C]ertain implementations of encryption pose an undeniable and growing threat to our ability to protect the American people. Our inability to access such data can stop our investigations and prosecutions in their tracks.”

FOREIGN REACH OF SCA ORDERS

EXTRATERRITORIAL APPLICATION IS NOT SETTLED.

BRACEWELL

Google told to hand over foreign emails in FBI search warrant ruling

Posted Feb 4, 2017 by Natasha Lomas (@riptari)

Tech titan pals back up Google after 'foreign server data' FBI warrant ruling

Means providers'll be 'forced to violate foreign privacy law'

TECHNOLOGY NEWS | Sun Feb 5, 2017 | 5:59am EST

Google, unlike Microsoft, must turn over foreign emails: U.S. judge

RULE 41 OF THE FEDERAL RULES OF CRIMINAL PROCEDURE

- (b) At the request of a federal law enforcement officer or an attorney for the government:
  - (1) a magistrate judge . . . may issue a warrant for property that is located outside the jurisdiction of any state or district, but within any of the following:
    - (A) **a United States territory, possession, or commonwealth**

  - (6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if:
    - (A) the district where the media or information is located has been concealed through technological means; or
    - (B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.

MICROSOFT DECISION AND THE GOOGLE RULING

- The Second Circuit's majority opinion relied on the "presumption against extraterritorial application of U.S. statutes" as articulated in *Morrison v. Nat'l Australia Bank Ltd.,* 561 U.S. 247 (2010).
- The Second Circuit analyzed the SCA and application of Section 2703 orders to material stored on foreign servers in light of the two-part approach set forth in *Morrison*:
  - whether the statute's warrant provisions contemplated extraterritorial application; and
  - the statute's focus.
- Ultimately, the Second Circuit concluded that the SCA focuses on user privacy and directing Microsoft to seize its customers communications stored overseas would be an unlawful extraterritorial application.
- Judge Rueter rejected the Second Circuit's application of *Morrison*, and further called into question the Second Circuit's conclusion that retrieval of documents stored on a foreign server constitutes a seizure in a foreign country.

IN RE XXXXXXXXXXXXXXXXX@YAHOO.COM (M.D. FLA)

- Geographic scope of the warrant lacked:
  - Nationality of Yahoo's customer
  - Location of customer when account was established
  - Customer's current location
  - Location of stored information being sought by the government
- Warrant sought "all information – including data stored outside of the United States – pertaining to the identified account that is in the possession, custody, or control of Yahoo."
- "[A] warrant issued pursuant to the Stored Communications Act reaches only as far as the territorial bounds of the United States . . . [i]f Yahoo has responsive information that is stored at a place outside the United States, it is not required to produce that information."

IN RE INFORMATION ASSOCIATED WITH ONE YAHOO ACCOUNT (E.D. WIS.)

- Warrant sought "all responsive information – including data stored outside the United States – pertaining to the identified account that is in the possession, custody, or control of Yahoo."
- "Rule 41 is silent as to whether a federal court may issue a warrant for search of property outside of the United States."
- "[E]ffect of an order under the SCA is to compel the service provider to disclose information in its possession. . .[i]t is not an authorization for government agents to physically enter any location or to seize anything from either the user or the service provider."

VIRTUAL CURRENCY & THE IRS

RESPONDING TO A JOHN DOE SUBPOENA

BRACEWELL

Department of Justice

Office of Public Affairs

SHARE

FOR IMMEDIATE RELEASE

Wednesday, November 30, 2016

Court Authorizes Service of John Doe Summons Seeking the Identities of U.S. Taxpayers Who Have Used Virtual Currency

Is The IRS Justified In Demanding Information On Millions Of Bitcoin Users?

Bitcoin Tax Fight Brews as Digital Chamber Set to Battle IRS

by **Matthew Leising**

March 8, 2017 9:00 AM *Updated on* March 8, 2017 1:48 PM

BRACEWELL

INFORMATION SOUGHT FOR YEARS 2013-2015

- User profile, history of changes to the user profile from account inception, user preferences, user security settings and history (including confirmed devices and account activity), payment methods and other information related to funding sources for the account.
- Records associated with Know-Your-Customer due diligence.
- Powers of attorney and other agreements or instructions for any account giving a third party access to or control of the account.
- Records of payments to and from the Coinbase account user.
- Account activity/transaction logs reflecting: date, amount, transaction type, account post-transaction balance, requests or instructions to send or receive bitcoin, name or identifier of the counterparty.
- Payments processed for which Coinbase acts as the payment service provider.
- Correspondence between Coinbase and its users.
- Periodic account statements or invoices.
- Exception reports produced by Coinbase's Anti-Money Laundering system.

JOHN DOE SUBPOENA – 26 U.S.C. § 7609

- A summons that does not identify the person with respect to whose liability the summons is issued.
- IRS is authorized to issue a John Doe summons pursuant to an investigation of a specific, unidentified person or ascertainable group or class of persons.
- Permits the IRS to obtains the names and requested information and documents concerning all taxpayers in a certain group or class of persons.
- Cannot be used to conduct a “fishing expedition.” The Service should be prepared to investigate the tax liabilities of specific taxpayers based on the information received from the John Doe summons.

REQUIREMENTS FOR OBTAINING A JOHN DOE SUBPOENA

- District Court approval is required before serving a John Doe Summons. Typically approved in an *ex parte* proceeding.
- Three specific requirements:
  - The summons must relate to the investigation of a **particular person or ascertainable group or class of persons.**
  - The IRS must have **a reasonable basis** for believing that such person or group or class of persons may fail or may have failed to comply with any provision of the tax laws.
  - The information and identities sought to be obtained from summoned records **must not be readily available from other sources.**

THE AGENCY SUBPOENA

KNOWING WHEN TO RESPOND

BRACEWELL

Twitter Sues Homeland Security To Protect Anonymity Of 'Alt Immigration' Account

April 6, 2017 · 7:22 PM ET

CAMILA DOMONOSKE

Twitter sues to stop Trump's team from unmasking whoever runs this anti-Trump account

TWITTER V. DEPT. OF HOMELAND SECURITY AND U.S. CUSTOMERS AND BORDER PROTECTION – THE ADMINISTRATIVE SUMMONS

- Issued pursuant to 19 U.S.C § 1509 which authorizes production of records related to the importation of merchandise.

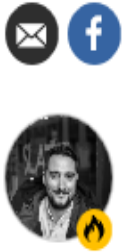
- The Summons:
  - Requested all records regarding the Twitter accounts @ALT_USCIS, including, user names, account login, phone number, mailing address and I.P. address.
  - Cautioned that failure to comply would result in proceedings in U.S. District Court to enforce the summons and possible sanctions.
  - Requested that Twitter non disclose the existence of the summons for an indefinite period of time.

OTHER NOTEWORTHY CASES

EMERGING ISSUES INVOLVING TECHNOLOGY & LAW ENFORCEMENT

BRACEWELL

Feds Walk Into A Building, Demand Everyone's Fingerprints To Open Phones



Thomas Fox-Brewster, FORBES STAFF

I cover crime, privacy and security in digital and physical forms. **FULL BIO**

BORDER SEARCHES

- The New York Times reported, in March 2017, that, in the wake of heightened scrutiny at border crossings (i.e., airports), individuals were reporting searches of their gadgets and devices.

- DHS enacted restrictions impacting travelers from 8 Muslim-majority countries who cannot bring devices larger than cell-phones on the plane (other devices must be stored in checked luggage).

- Airlines are cautioning international travelers to have their devices charged and accessible by Border Agents; travelers could be detained until agents can search devices.

Man suspected in wife's murder after her Fitbit data doesn't match his alibi

Officials say the timeline given by Richard Dabate, accused of killing his wife in their Connecticut home, is at odds with data collected by her wearable device

Amazon Echo search warrant could spur new prosecution methods, expert says

Originally published January 3, 2017 at 6:00 am | *Updated January 2, 2017 at 2:59 pm*

QUESTIONS?

PHILIP J. BEZANSON

SHANNON B. WOLF

This presentation is provided for informational purposes only and should not be considered specific legal advice on any subject matter. You should contact your attorney to obtain advice with respect to any particular issue or problem. The content of this presentation contains general information and may not reflect current legal developments, verdicts or settlements. Use of and access to this presentation does not create an attorney-client relationship between you and Bracewell.

BRACEWELL