[redacted] (INSD) (FBI)

From: THOMAS, JULIE F. (OGC) (FBI)
Sent: Tuesday, December 19, 2006 8:53 AM
To: [redacted]INSD) (FBI)
Cc: [redacted] (OGC) (FBI)
Subject: FW: OIG Request for all OGC Guidance on 2702 letters

b6 b7C **UNCLASSIFIED**
NON-RECORD

Dear [redacted]

Could you process the attachments for the OIG?

Thanks,
Julie

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Monday, December 18, 2006 9:24 AM
b6 b7C **To:** [redacted] (OGC) (FBI); LAMMERT, ELAINE N. (OGC) (FBI); [redacted] (OGC) (FBI); THOMAS, JULIE F. (OGC) (FBI)
Subject: RE: OIG Request for all OGC Guidance on 2702 letters

UNCLASSIFIED
NON-RECORD

In response to the OIG request, attached is additional guidance detailed below.

1 - The original guidance on the Patriot Act issued in 2002 included a paragraph addressing the newly created emergency disclosure provision.

2 - An e-mail sent to all CDCs advising on the use of forms generated by ISPs for emergency disclosures. (I am not able to attach this, however, I included a copy of the e-mail below.)

3 - EC to the field seeking a report on all emergency disclosures received in order to respond to the provisions in the Homeland Security Act which added a one year reporting requirement.

Feel free to contact me if there are any questions.

[redacted]
ILU - x[redacted]

b6 b7C b2


rLD_GD.WPD (49 KB)


EC April 2702 eport.wpd (19 K.

From: [redacted] (OGC) (FBI)
Sent: Thursday, November 17, 2005 1:55 PM
b6 b7C **To:** FBI_ALL CDCs
Cc: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] R. (OGC) (FBI)
Subject: Emergency Disclosure Forms from ISPs

UNCLASSIFIED
NON-RECORD

A recent EC established policy that ASAC (or higher) approval is required to voluntarily obtain both content and records from a service provider under the emergency disclosure provision in 18 USC 2702 (b)(8) & (c)(4). (See attached EC below.) The EC cautioned that many ISPs are requiring the SA to sign an emergency disclosure form that states the SA will follow up with "the appropriate documentation (i.e. subpoena, court order, search warrant)." As the EC states, disclosures under the emergency disclosure provision do not require additional legal process, to do so then turns it from a voluntary disclosure under 2702 to a compelled disclosure under 2703. Should a SA sign such a form in the midst of an emergency, I encourage offices to follow up the emergency disclosure with a letter from the FBI requesting the emergency disclosure in accordance with the emergency disclosure provision instead of seeking a subpoena or other compelled process. A sample letter is attached to the EC. OGC believes that this fulfills any obligation the form may create to provide the "necessary or appropriate documentation."

As always, should you have any questions, please feel free to contact me.

[redacted]
b6 Assistant General Counsel
b7C Investigative Law Unit
Office of the General Counsel
b2 (202) 324-[redacted]

2702
idance.wpd (46 k

-----Original Message-----
b6 **From:** [redacted](OGC) (FBI)
b7C **Sent:** Thursday, December 14, 2006 4:59 PM
To: LAMMERT, ELAINE N. (OGC) (FBI); [redacted](OGC) (FBI); [redacted](OGC) (FBI); THOMAS, JULIE F. (OGC) (FBI)
Subject: FW: OIG Request for all OGC Guidance on 2702 letters

UNCLASSIFIED
NON-RECORD

<< File: 2702A.WPD >> << File: 2702B.WPD >> << File: 2702disc-DOJ-rpt.pdf >>
<< File: 2702C.WPD >> << File: 2702D.WPD >>

This is the stuff that I have. 2702A is guidance from cyber that goes over all the means of obtaining information from ISP's, [redacted] helped write it and it references emergency disclosures. 2702B is guidance that ILU recently wrote establishing a process for meeting the congressional reporting requirments established by the Patriot Renewal Act, the PDF is the DOJ attachment that goes with this ec. 2702C is the guidance that [redacted] wrote regarding the Patriot Act renewal that references the emergency disclosure provisions. 2702D is the 8/25 ec from ILU with guidance on these disclosures that I think you already have.

[redacted]

-----Original Message-----
From: THOMAS, JULIE F. (OGC) (FBI)
b6 **Sent:** Thursday, December 14, 2006 3:16 PM
To: LAMMERT, ELAINE N. (OGC) (FBI)
b7C **Cc:** [redacted](OGC) (FBI); [redacted]OGC) (FBI)
Subject: OIG Request for all OGC Guidance on 2702 letters

UNCLASSIFIED
NON-RECORD

As part of the NSL OIG review, OIG is requesting all OGC guidance on the use of 2702 Patriot Act letters. I have the EC we did on 8/25/2005. Is there anything else we can/should provide?

Thanks,

Julie F. Thomas
DGC, National Security Law Branch
Office of the General Counsel
Room 7975
b2 *202-324* [redacted]
202-324 [redacted] *(fax)*
[redacted]

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: IMMEDIATE **Date:** 04/15/2003

To: All Field Offices **Attn:** ADIC
SAC
CDC

From: Office of the General Counsel
Investigative Law Unit/Room
Contact:

b6
b7C
b2

Approved By: Kelley Patrick W
Lammert Elaine N

Drafted By:

Case ID #: 66F-HQ-1085160 (Pending)
66F-HQ-1085159 (Pending)
66F-HQ-C1382989 (Pending)
66F-HQ-C1384970

Title: Emergency Disclosures under ECPA
18 U.S.C. § 2702
Reporting Requirement

Synopsis: This EC advises receiving field offices of the reporting requirement under 18 U.S.C. Section 2702(b)(7) regarding any voluntary disclosures made by a service provider to the FBI under this emergency disclosure provision. Field offices must immediately report if they received any voluntary disclosures of content or records from service providers under this provision between January 24, 2003 and March 31, 2003. Negative reports are not required. Additional reports will be required at later dates.

Enclosure(s): Sample report

Details: The Electronic Communications Privacy Act (ECPA), codified in 18 U.S.C. § 2701, *et. seq.*, provides privacy protection for electronic communications, such as e-mail, and associated records. It also outlines the compulsory process that law enforcement can use to obtain both the content of communications and records held by an electronic communications service provider or a remote computing service, most often an Internet Service Provider (ISP). The USA Patriot Act created a voluntary disclosure provision which explicitly permits, but does not require, a service provider to disclose to law enforcement either content or non-content customer records in emergencies involving an immediate risk of death or serious physical injury to any person. 18 U.S.C. § 2702(b)(7); 18 U.S.C. § 2702(c)(4). The Homeland Security Act modified this provision and created a reporting requirement for every disclosure made under this provision.

This EC provides guidance on the reporting requirement and notifies the field of urgent deadlines in order to ensure full compliance with the statutory deadlines. Further guidance will be issued in the near future on the use of the provision.

The reporting requirement as enacted in the Homeland Security Act reads as follows:

> "A government entity that receives a disclosure under section 2702(b) of title 18, United States Code, shall file, not later than 90 days after such disclosure, a report to the Attorney General stating the paragraph of that section under which the disclosure was made, the date of the disclosure, the entity to which the disclosure was made, the number of customers or subscribers to whom the information disclosed pertained, and the number of communications, if any, that were disclosed. The Attorney General shall publish all such reports into a single report to be submitted to Congress 1 year after the date of enactment of this Act."[1]

While the language of the reporting requirement states that any disclosure to the government under 18 U.S.C. § 2702(b) must be reported, a reasonable interpretation of the legislative history narrows this reporting requirement to 2702(b)(7), the emergency disclosure provision.[2] This is a one-time reporting requirement, meaning that after the Attorney General files the report in November 2003, the reporting requirement ceases.

Generally, when the FBI seeks information from an ISP, the request will be directed at a certain account or on-line identity (i.e., screen name). One subscriber may have multiple accounts and each account may include multiple identities. We may be unable to distinguish accounts and identities from customers and subscribers until well into the investigation. Therefore, to satisfy the reporting requirement and to simplify the reporting process, the FBI will report the number of accounts or identities about which information was sought, instead of the number of customers or subscribers. For example, if in responding to a crisis surrounding a kidnaping the FBI has five e-mail addresses for which information is sought, then even if all five addresses are held by the same person, the FBI will report that information was sought pertaining to five e-mail addresses. Similarly, if one letter to an ISP lists four screen names and five e-mail addresses, then the FBI will report that information was sought on nine identities. In the cover letter to the report we will explain what the data means and why we

---

[1]Homeland Security Act of 2002, P.L.107-296, § 225(d)(2).

[2]§ 2702(b) authorizes the ISP to make disclosures to the intended recipient of the e-mail, consistent with the consent of the originator or recipient, and to another service used to forward the mail to the intended recipient. Congress did not intend for the Attorney General to report to Congress every time that a government employee receives an e-mail that was forwarded through an ISP. The legislative history demonstrates that Congress' concern was that law enforcement might abuse the ability to approach an ISP and present emergency circumstances to the ISP, causing the ISP to voluntarily provide e-mail content and records to the law enforcement agency. It is only in this context that the reporting requirement is discussed in the legislative history. See H.R. Rep. 107-497, pg. 14; 148 Cong. Rec. H4580-05, pg. H4583 (Congressional debate on the Cyber Security Enhancement Act of 2002, dated July 15, 2002)(statement of Ms. Jackson-Lee).

cannot report the exact information requested. By reporting and explaining this information, the FBI will be complying with the intent of the law.

To facilitate the reporting process, the Investigative Law Unit (ILU), Office of the General Counsel (OGC) will act as the central point for all FBI reports of disclosures under the emergency disclosure provision. Field offices should provide ILU with a list of the disclosures they have received under this provision. Information should be submitted in the form of an Excel spreadsheet with one column each for the following information: 1) the date of receipt of the disclosure; 2) whether content (i.e., e-mail) or records were received; and 3) the number of e-mail messages or communications disclosed. A separate record or line item should be listed for each account or identity about which the disclosure was made. A sample spreadsheet is attached.

The statute requires that disclosures made under this emergency disclosure provision are to be reported to the Attorney General within 90 days of the disclosure. As a part of the Homeland Security Act, the reporting requirement became effective on January 24, 2003. Therefore, any disclosures received prior to January 24, 2003, need not be reported. Any disclosures made under § 2702(b)(7) and received on January 24, 2003, must be reported to the Department of Justice (DOJ) by April 24, 2003. In order to provide this information to the DOJ within the deadline, any office which received disclosures under this emergency disclosure provision between January 24 and March 31, 2003 are to: 1) telephonically notify Assistant General Counsel (AGC [redacted] ILU, OGC at (202) 324-[redacted] or [redacted] ILU, OGC (202) 324-[redacted] as soon as possible; and 2) submit the above detailed information to ILU by April 21, 2003 so that any necessary reporting can be made to the DOJ within the statutory deadlines. Negative reporting is not required.

b6
b7C
b2

Thereafter, reports should be submitted quarterly (via EC with an electronic copy also sent via e-mail) under the following schedule: all disclosures received between April 1 and June 10, 2003 are to be reported to ILU by June 20, 2003; all disclosures received between June 11 and August 15, 2003 are to be submitted to ILU by August 31, 2003; all disclosures received between August 16 and October 15, 2003 are to be submitted to ILU by November 1, 2003.

Any questions should be directed to AGC [redacted] at telephone number (202) 324-[redacted] or UC Elaine Lammert at (202) 324-[redacted]

LEAD(s):

Set Lead 1: (Action)

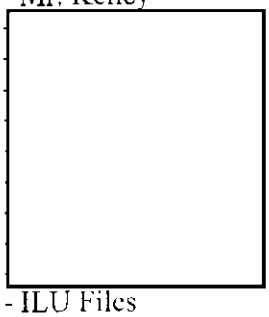
ALL RECEIVING OFFICES

Any office which has received a disclosure of electronic communications or records from a service provider under 18 U.S.C. § 2702 since January 24, 2003 are to telephonically notify the above contact person immediately and provide a written report of such disclosures in accordance with the dates specified above. Negative reports are not required.

♦♦

cc: 1 - Mr. Kelley

b6
b7C



2 - ILU Files