Electronic Frontier Foundation
Protecting Rights and Promoting Freedom on the Electronic Frontier

October 12, 2007

VIA FACSIMILE AND MAIL

The Honorable John D. Dingell
Chairman of the Committee on Energy and Commerce
The Honorable Edward J. Markey
Chairman of the Subcommittee on Telecommunications and the Internet
The Honorable Bart Stupak,
Chairman of the Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
United States House of Representatives
2125 Rayburn House Office Building,
Washington, DC 20515

Re: Concerns with the Public Law 110-55, the Protect America Act of 2007

Dear Honorable Chairmen:

Thank you for the opportunity to provide you with information in response to your letter of October 2, 2007 regarding potential implications of Public Law 110-55. I am the Legal Director of the Electronic Frontier Foundation (EFF), a donor-supported non-profit membership organization that works to inform policymakers and the general public about civil liberties issues related to technology, and acts as a defender of those liberties. As such, EFF has been closely following the debate surrounding Public Law 110-55 as well as ongoing efforts to fix that deeply flawed statute with additional legislation. We are delighted to have the opportunity to respond to your questions.

EFF has also been active in the fight against illegal warrantless dragnet surveillance in the courts. On January 31, 2006, EFF filed a class-action lawsuit against AT&T (*Hepting v. AT&T*, N.D. Cal. Case No. C-06-0672-VRW)[1] accusing the telecom giant of violating the law and the privacy of its customers by collaborating with the National Security Agency (NSA) in its massive and illegal program to wiretap and data-mine the communications of ordinary Americans. In order to assist the Committee in evaluating AT&T's response to its October 2, 2007 letter to AT&T, we summarize below some of the evidence submitted to the United States District Court for the Northern District of California in that litigation.

We also note that this Committee has asked several telecommunications companies about their responses to FBI letters seeking information about a subscriber's "community of interest." In March 2007, EFF filed a Freedom of Information Act

[1] For complete information about the litigation, please visit http://www.eff.org/legal/cases/att/.

454 Shotwell Street • San Francisco, CA 94110 USA
+1 415 436 9333 +1 415 436 9993 www.eff.org information@eff.org

lawsuit seeking fundamental information about the FBI's misuse of National Security Letters. On June 16, 2007, a federal judge ordered the FBI to process 2,500 pages a month responsive to EFF's request.[2] Included in the response were several so-called "exigent letters" seeking community of interest information, which subsequently became the subject of the *New York Times* articles to which this Committee referred in Question 13.[3] To assist this Committee in understanding the legal issues surrounding the exigent letters, we include a short summary of our legal concerns about these demands.

I. Responses to the Committee's Questions.

A. The Effect That Increasing the Number of Databases of Personal Information Maintained by the Government May Have on the Risk of Breach of those Databases.

Increasing the number of databases containing personal information that are maintained by (or are directly accessible by) the government increases the risk of improper access to those databases, including by breach. Simply put, increasing the number of databases introduces more points of vulnerability into the system, and increases the chance that the databases (as well as the networks accessing the databases) may become pregnable to attackers who want to steal Americans' data or personal information.

The security weaknesses in government databases are already well known; indeed, federal data breaches occur quite often. For example, a survey by the House Government Reform Committee revealed more than 788 breaches of federal databases between January 2003 and July 2006. U.S. Government Accountability Office, *Personal Information: Data Breaches are Frequent, but Evidence of Identity Theft is Limited; However, Full Extent is Unknown* 13-14, GAO-07-737 (June 2007). Furthermore, the U.S. Computer Emergency Readiness Team, a Department of Homeland Security component that oversees federal government computer security matters, documented 477 database breaches within 59 federal agencies and contractors during fiscal year 2006 alone. *Id.* at 13-14. Likewise, a March 2007 audit revealed that at least 490 Internal Revenue Service laptop computers containing taxpayer information had been lost or stolen since 2003. *Id.* at 14.

The potential risk posed to individuals by such breaches is particularly troubling when portions of key national security databases have been exempted from critical provisions of the Privacy Act, including the requirement that agencies collect only information that is "relevant and necessary to accomplish a purpose of the agency

---

[2] For more information about this litigation, please see http://www.eff.org/flag/07656JDB/.

[3] Examples of such letters are available online at http://www.eff.org/flag/07656JDB/080607_exigent_letters_coi.pdf.

required to be accomplished by statute or by Executive order of the President."[4] Federal agencies are also known to have collected and maintained massive amounts of information from the private sector, in some cases without any legal basis.[5]

Moreover, using multiple connected databases can make it harder to monitor privacy compliance. There are two basic problems. First, information sharing between databases is rarely transparent, which can lead to various types of inaccuracies: individuals' names may not be consistent across databases (e.g., "John Doe," "Doe, John," "J. Doe," "John Q. Doe"); different individuals may share a common name; different databases may have different quality and security protocols.

Problems are common even in single databases. The Department of Justice Office of the Inspector General ("OIG") report on the FBI's National Security Letter ("NSL") problems revealed that the central Federal Bureau of Investigation ("FBI") Office of General Counsel database contained much incomplete or inaccurate information about NSL issuance.[6] Much data was not entered in timely fashion, and some of the entries were erroneous. As a result, the FBI's NSL reporting was inaccurate, and the database problems prevented OIG from conducting an accurate audit.

Second, when information is shared between databases, it can be much harder to correct errors, especially if the data flows are not carefully logged. Correcting an error in one database may not correct that error in other databases, and the error can even propagate back to the corrected database. Even information that was initially correct can become stale and require updating. A good example is the Terrorist Screening Database (TSDB), which receives information from various agency source databases and sends

---

[4] *See, i.e.*, EFF's recent comments discussing this problem with respect to the Automated Targeting System, Secure Flight Records System, and Terrorist Screening Records System, http://www.eff.org/Privacy/travel/.

[5] For a discussion of such instances of data sharing, *see, e.g.*, Letter from Cathleen A. Berrick, Director, Homeland Security and Justice Issues, U.S. Government Accountability Office, to Congressional Committees: *Aviation Security: Transportation Security Administration Did Not Fully Disclose Uses of Personal Information During Secure Flight Program Testing in Initial Privacy Notices, but Has Recently Taken Steps to More Fully Inform the Public* (July 22, 2005); U.S. Department of Homeland Security Privacy Office, *Secure Flight Report: DHS Privacy Office Report to the Public on the Transportation Security Administrations Secure Flight Program and Privacy Recommendations* (Dec. 2006); U.S. Department of Homeland Security Privacy Office, *Report to the Public on Events Surrounding JetBlue Data Transfer: Findings and Recommendations* (Feb. 20, 2004).

[6] U.S. Dept. of Justice, Office of the Inspector General, *A Review of the Federal Bureau of Investigation's Use of National Security Letters* 32-36 (March 2007).

information to downstream screening agency databases[7] and has well-documented accuracy and redress problems.[8] Thus, monitoring for privacy compliance may require the significant effort of analyzing each connected agency's practices.[9]

B. The Likelihood that the Government Might Use Information From Those Databases for Purposes Other Than Those For Which It Was Originally Collected.

Unfortunately, there has not been reasonable assurance that the government will appropriately safeguard the privacy and security of information in such databases, and will ensure that no one accesses information that is not authorized to be collected. Where covert surveillance is at issue, we must ask, "who will watch the watchers?" Given the failures uncovered by the OIG in the abuse of the National Security Letter power, we cannot ignore the severe risk that direct access to databases of information about private American citizens will also be abused.

As the Department of Defense's Technology and Privacy Advisory Committee (TAPAC) explained, "mission creep" [10] is a serious risk associated with the government's appetite for personal information and modern data-mining technology.[11] The risk that information collected for one purpose will be used for another is "particularly acute . . . when the use of personal data about U.S. persons is justified by an extraordinary need such as protecting against terrorist threats," and "consistent experience . . . suggests that,

---

[7] U.S. Dept. of Justice, Office of the Inspector General, *Follow-up Audit of the Terrorist Screening Center* 5, Audit Report 07-41 (Sept. 2007), Exhibit 1-1 (Terrorist Watchlist Dataflow Diagram).

[8] *Id.* at 25 ("the TSC has not yet implemented routine processes to ensure that the TSDB contained all proper watchlist nominations and did not contain duplicate data resulting from improperly processed records, system malfunctions, and historical data deficiencies. Moreover, despite being responsible for removing outdated or obsolete data from the TSDB, the TSC did not have a process for regularly reviewing and verifying the contents of the TSDB. . . . Finally, because of internal FBI watchlisting processes, the TSC cannot ensure that accurate and complete terrorist information has been disseminated to downstream screening systems in a timely manner").

[9] The FBI's practices were particularly problematic. *Id.* at 18-19.

[10] For example, the government may use an airline passenger's request for a special meal to determine the passenger's religious affiliation. *Safeguarding Privacy in the Fight Against Terrorism*, Report of the Technology and Privacy Advisory Committee 39 (March 2004).

[11] Other risks identified by TAPAC include: "chilling effect and other surveillance risks," *id.* at 35; "data aggregation risks," *id.* at 36; "data inaccuracy risks," *id.* at 37; "false positives," *id.* at 39; and "data processing risks" such as disclosure, data misuse, data transfer, data retention, and insecurity, *id.* at 40-42.

over time, there is always pressure to use data collected for one purpose for other purposes."[12] Moreover, these privacy risks "are only likely to increase as information technologies develop."[13] TAPAC accordingly warned that the government must "enact appropriate legal, technological, and managerial safeguards to minimize those risks and protect against misuse."[14]

II. Evidence of AT&T's Installation of Interception Equipment

In Question 12 of its letters to telecommunications providers, the Committee asks about the telecommunications providers' roles in facilitating the interception of communications by installing or permitting the installation of equipment on their networks to intercept Internet traffic.

To assist the Committee with its investigation, we summarize below the evidence showing AT&T's role in the installation of equipment to facilitate wholesale interception of Internet traffic.[15] This evidence has been submitted to the court in *Hepting v. AT&T*, N.D. Cal. Case No. C-06-0672-VRW.[16]

A. AT&T's San Francisco Interception Facility

The *Hepting* case began when a former AT&T employee named Mark Klein came forward with detailed eyewitness testimony and documentary evidence proving that AT&T has been collaborating with the NSA in the surveillance of the domestic communications of millions of Americans. Mr. Klein had worked as an AT&T technician for 22 years, most recently at AT&T's San Francisco switching facility on Folsom Street. He described events and operations he had observed at AT&T in a sworn declaration laden with self-verifying detail and supported by AT&T's own documents.[17]

Mr. Klein's account begins around January 2003, when the manager of his facility advised him that the NSA was coming to interview another colleague for a "special job." The "special job" was to install equipment in a high-security room AT&T was building at

---

[12] Id. at 39-40 ("The expansive uses to which Social Security Numbers have been put are a practical example.").
[13] Id. at 42.
[14] Ibid.
[15] This letter focuses on the declaration and documents submitted as evidence in litigation. In addition the Committee may find it helpful to review a summary of key news articles regarding AT&T's role in warrantless surveillance, available at http://www.eff.org/legal/cases/att/news.php.
[16] For complete information about the litigation, please visit http://www.eff.org/legal/cases/att/.
[17] The declaration of Mark Klein is available at http://www.eff.org/legal/cases/att/SER_klein_decl.pdf.

its Folsom Street Facility. The NSA supervised the construction and outfitting of the room, which came to be known as the "SG3 Secure Room." Mr. Klein personally saw the room when it was under construction, and, at one point, entered the room briefly after it was fully operational.

In October 2003, AT&T transferred Mr. Klein to the Folsom Street Facility. Although AT&T entrusted Mr. Klein with keys to every other door at the Folsom Street Facility, he did not have access to the SG3 Secure Room. No AT&T employee was allowed in the secret room without NSA security clearance.

Mr. Klein recounts one event that underscores the "extremely limited access to the SG3 Secure Room": A large industrial air conditioner in the room began "leaking water through the floor and onto ... equipment downstairs." AT&T maintenance personnel were not allowed to enter to fix the leak—or even to triage and prevent water damage to other portions of the facility. Despite the "semi-emergency," AT&T waited days for a repairman with NSA clearance to provide service.

At the Folsom Street Facility, Mr. Klein's job was to oversee AT&T's "WorldNet Internet room." Communications carried by AT&T's WorldNet Internet service pass through that room to be directed to or from customers. The Folsom Street Facility also handles millions of telephone communications.

Mr. Klein revealed that AT&T intercepts every single one of the communications passing through the WorldNet Internet room and directs them all to the NSA. As Mr. Klein explained, the communications are carried as light signals on fiber-optic cables. To divert the communications, AT&T connected the fiber-optic cables entering the WorldNet Internet room to a "splitter cabinet." The splitter cabinet splits the light signals from the WorldNet Internet service in two, making two identical copies of the material carried on the light signal. The splitter cabinet directed one portion of the light signal through fiber optic cables into the NSA's secret room while allowing the other portion to travel its normal course to its intended destination. The split cables carried domestic and international communications of AT&T customers, as well as communications from users of other non-AT&T networks that pass through the Folsom Street Facility.

Mr. Klein attached to his declaration two AT&T documents called "SIMS Splitter Cut-In and Test Procedure," which describe "how to connect the already in-service circuits to a "splitter cabinet," which diverted light signals from the WorldNet Internet service's fiber optical circuits to the SG3 Secure Room."[18] He also attached a third AT&T document "describ[ing] the connections from the SG3 Secure Room on the 6th floor to the WorldNet Internet room on the 7th floor, and provid[ing] diagrams on how the light signal was being split." This document also "listed the equipment installed in

[18] The exhibits to the declaration of Mark Klein are available at http://www.eff.org/legal/cases/att/SER_klein_exhibits.pdf.

the SG3 Secure Room." These three documents comprise over 100 pages of highly technical details on the interceptions, including 57 detailed schematics and 24 tables of data.

AT&T has confirmed that the descriptive information presented by Mr. Klein is accurate. During the litigation, AT&T presented a declaration from James Russell, AT&T's Managing Director-Asset Protection, that confirmed that Mr. Klein's declaration and the AT&T documents Mr. Klein attached accurately describe AT&T's Internet network, AT&T's San Francisco communications facility and the location of specific equipment within the San Francisco facility, and the interconnection points of AT&T's Internet network with the networks of other communications carriers. Mr. Russell confirmed the conclusion that the exhibits to the Klein Declaration are authentic AT&T documents that provide "detailed schematics of network wiring configurations that are uniform across AT&T locations and that are used by AT&T to cross-connect and split fiber cables" and "identif[y] the manufacturer and name of many pieces of equipment used by AT&T."

The *Hepting* plaintiffs retained an expert in information technology and telecommunications to explain the implications of the documents and testimony Mr. Klein furnished. The expert, J. Scott Marcus, spent decades working for a variety of telecommunications clients, including working closely with AT&T. He also served as Senior Advisor for Internet Technology at the Federal Communications Commission. Mr. Marcus confirmed "Mr. Klein's allegation that the room described was a secure facility, intended to be used for purposes of surveillance on a very substantial scale."[19] He "conclude[d] that AT&T has constructed an extensive—and expensive— collection of infrastructure that collectively has all the capability necessary to conduct large scale covert gathering of IP-based communications information, not only for communications to overseas locations, but for purely domestic communications as well." "This deployment," he opines, "is neither modest nor limited."

The expert further concluded that "all or substantially all" of AT&T's "peered traffic" in San Francisco was sent into the SG3 Secure Room, meaning any communication between AT&T customers and non-AT&T customers. AT&T made no effort to filter out purely domestic-to- domestic electronic communications, as a fiber splitter is not a selective device; all traffic on the split circuit was diverted or copied.

B. AT&T Intercepts Communications in Other Cities

That was just in San Francisco. From the arrangement of the hardware, Mr. Marcus concluded that AT&T's surveillance "apparently involves considerably more locations than would be required to catch the majority of international traffic." Further

[19] The declaration of J. Scott Marcus is available at http://www.eff.org/legal/cases/att/SER_marcus_decl.pdf,

evidence confirms the expert's view. Mr. Klein reports "that other such 'splitter cabinets' were being installed in other cities, including Seattle, San Jose, Los Angeles and San Diego." Two former AT&T employees have revealed a similar secure room at an AT&T command center in St. Louis.[20] They report that "AT&T has maintained a secret, highly secured room since 2002 where government work is being conducted" and that "only government officials or AT&T employees with top-secret security clearance are admitted to the room."

According to Mr. Marcus, this web of surveillance facilities would probably capture well over half of AT&T's purely domestic traffic, representing almost all of the AT&T traffic to and from other providers. This comprises about "10% of all purely domestic Internet communications in the United States," including non-AT&T customers.

III. Legal Issues with Exigent Circumstances Letters

In Question 13 to the telecommunications providers, the Committee asks about the carriers' responses to government "exigent circumstances letters" seeking details on their customers' "communities of interest."[21] To assist the Committee in its investigation, we provide below a discussion of the laws relevant to such letters.

A. Background

As this Committee is aware, in March 2007, the OIG released a formal report (OIG Report) revealing that the Federal Bureau of Investigation (FBI)'s Communications Analysis Unit (CAU) had routinely been using "exigent letters" to obtain customer information from three telecommunications companies.[22] "Exigent letters" are informal requests (i.e. not subpoenas, warrants, court orders, or other statutory requests) that ask the telecommunications recipient provide "call detail records" about particular subscribers, and, in some letters, to also disclose the subscriber's "community of interest."[23] Disclosures of the subject's "community of interest" involve disclosures

---

[20] Kim Zetter, *Is the NSA spying on US Internet traffic?*, Salon (June 21, 2006), available at http://www.salon.com/news/feature/2006/06/21/att_nsa/index_np.html.

[21] The Committee's letter refers to National Security Letters. The letters seeking information about subscribers' communities of interest uncovered by EFF's FOIA litigation and reported in the *New York Times* were in "exigent circumstances" letters, that did even purport to be under the NSL authority. We presume that the telecommunications carriers will respond with respect to any "community of interest" letters, regarding of whether the letter was an exigent letter or an NSL.

[22] *See supra* note 6

[23] Examples of such letters are available online at http://www.eff.org/flag/07656JDB/080607_exigent_letters_coi.pdf.

about other subscribers who communicate with the subject of the request.[24] In many cases, the CAU issued exigent letters in non-emergency situations where there was no underlying investigation. OIG Report, at p. 93.

The OIG Report looked only at the time period between March 11, 2003 and December 16, 2005, and found 739 exigent letters, pertaining to approximately 3,000 telephone numbers. OIG Report, at pp. 89-90. According to the OIG Report, these exigent letter disclosures were performed pursuant to contracts with three telecommunications companies, though the disclosures went beyond the contract's written terms. OIG Report, at p. 90. News reports show that FBI pays the telecommunications providers "about $1.8 million a year to process written 'emergency' requests for telephone and Internet records."[25]

Subsequently, in testimony before the House Judiciary Committee, Valerie Caproni, General Counsel of the FBI, confirmed that the companies were AT&T, Verizon and MCI.[26] Following the OIG Report, the FBI claimed that it had discontinued the practice (as of March 5, 2007).[27] The OIG is continuing its investigation.

B. "Exigent Letters" Violate the Law

Federal and state laws carefully regulate the circumstances under which a telecommunications provider may disclosure call detail records of a subscriber. As the OIG Report found (OIG Report at p. 96), there is no legal basis for the providers to reveal customer information in response to an "exigent circumstances letter."

To help clarify that issue, this memo will briefly outline the relevant laws. As an initial matter, the Telecommunications Act, 47 U.S.C. § 605 provides that:

> (a) Practices prohibited – Except as authorized by chapter 119, Title 18, no person receiving, assisting in receiving, transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof, except through authorized channels of transmission or reception, (1) to any person other than the addressee, his agent, or attorney, (2) to a person employed or authorized to forward such communication to its destination, (3) to proper accounting or distributing officers of the various communicating centers over which the communication may be passed, (4) to the master of a

[24] See news report at http://www.nytimes.com/2007/09/09/washington/09fbi.html.
[25] See news report at http://blog.wired.com/27bstroke6/2007/07/fbi-unit-that-l.html.
[26] See news report at http://blog.wired.com/27bstroke6/2007/03/fbi_confirms_co.html.
[27] See DOJ press release at http://www.usdoj.gov/opa/pr/2007/March/07_nsd_168.html.

> ship under whom he is serving, (5) in response to a subpoena issued by a court of competent jurisdiction, or (6) on demand of other lawful authority.

In addition, 47 U.S.C. § 222 provides for the confidentiality of customer proprietary network information (CPNI).[28] In relevant part, Section 222 states:

> (c) Confidentiality of customer proprietary network information – (1) Privacy requirements for telecommunications carriers – Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.

Thus, the Telecommunications Act provides a general rule of confidentiality, and only allows for disclosure "on demand of other lawful authority" or "as required by law." In other words, without a statutory exception that demands or requires disclosure, telecommunications carriers are forbidden from disclosing the information sought by the "exigent letters." As explained below, no other lawful authority permits (or requires) the exigent letter disclosures reported by the OIG.

The Stored Communications Act, 18 U.S.C. § 2701 *et seq.*, (which was enacted as part of the Electronic Communications Privacy Act of 1986), also puts strict limits on when a telecommunications provider can hand over customer data to the government. Section 2702(A)(1) prohibits disclosure of the contents of a communication, and (A)(3) forbids the release of a "record or other information pertaining to a subscriber to or customer" other than the content covered by (A)(1). Thus, sections 2702(A)(1) and (A)(3) compliment one another, and together protect all records about a communication.

Again, absent a specific statutory exception, it is illegal for the telecoms to provide customer information to the government. Section 2703 sets forth the various methods by which the government may obtain access to subscriber information. For example, certain basic subscriber information may be obtained with an "administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial

---

[28] For more information about CPNI, see http://www.fcc.gov/cgb/consumerfacts/phoneaboutyou.html.

subpoena." 18 U.S.C. § 2703(b)(1)(B)(i). However, this list does not include exigent letters.[29]

According to the OIG report, the FBI's legal counsel attempted to justify the "exigent letters," under 18 U.S.C. § 2702(c)(4), which permits a telecommunications provider to disclose records "to a governmental entity, if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information."[30] *See* OIG Report, p. 94.[31]

To the contrary, the OIG found that the letters were in fact used in mostly non-emergency situations. In addition, as the OIG explained, this "emergency voluntary disclosure provision" was not actually relied upon by the government in making these requests, and in any event, "the letters did not recite the factual predication necessary to invoke that authority."

The primary open legal and factual question is whether or not Verizon and AT&T had the required reasonable belief of an emergency for each affected customer in the over 700 "exigent letters" requesting information on approximately 3,000 telephone numbers.

In the media, both Verizon and AT&T have insisted that they only responded to what they believed were emergency requests.[32] While it seems unlikely that the telecommunications companies had the required reasonable belief for the direct subject of the "exigent circumstances letter," it will be even harder for them to show that they were able to form such a belief for the customers in the "community of interest" surrounding the subject of the letter based only on a form letter containing the word "exigent."

---

[29] The text of the letters often noted that a subpoena request had been presented to the U.S. Attorney's Office, and promised to supply the subpoena later. The OIG Report found that this was factually inaccurate, and could not find one instance in which the subpoena request had actually been submitted prior to the exigent letter. After the OIG Report, the FBI has attempted to provide after the fact legal process for at least some exigent letters.

[30] In 2006, the Patriot Reauthorization Act, Pub.L. 109-177, § 107(b)(1)(B) replaced this language with "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." All of the exigent letters covered by the OIG Report were prior to this language change. For letters after the language change, the telecommunications provider would still have the high burden of showing good faith.

[31] See also FBI Director Mueller March 27, 2007, statement to the Senate Judiciary Committee, http://www.fbi.gov/congress/congress07/mueller032707.htm (raising same argument).

[32] See news report at http://blog.wired.com/27bstroke6/2007/03/att_verizon_we_.html.

Only one court has considered 18 U.S.C. § 2702(c)(4)'s exception for emergency records disclosure at any length. That court, in declining to apply the exception, reached the only conclusion that the plain language of the exception allows: that the emergency exception is reserved for voluntary disclosures in response to specific and urgent emergencies, and that it is the burden of the defendant to prove the exception's applicability. *See Freedman v. America Online, Inc.*, 303 F. Supp. 2d 121, 127-28 (D. Conn. 2004).

Generalized fears are not sufficient to support a reasonable belief in an immediate emergency threat to life or limb. Instead, the emergency exception is reserved for specific emergency situations "in which time is of the essence and requiring that a court order be obtained would cause delay which could result in severe jeopardy for a victim of crime." *In re Application of U.S. for Nunc Pro Tunc Order for Disclosure of Telecom. Records*, 352 F. Supp. 2d 45, 47 (D. Mass. 2005) (declining to issue retroactive court order authorizing telecommunications provider's voluntary disclosure of records concerning a kidnapping for ransom because the statute does not provide for such orders, opining in dicta that such an order was unnecessary to shield the provider from potential liability because its conduct fit the emergency exception). *See also U.S. v. Crouch*, 666 F. Supp. 1414, 1416-17 (N.D. Cal. 1987) (in a Wiretap Act case, holding that reliable information that suspects with violent records were planning a bank robbery sometime in the next 60 days *did not* suffice to establish an emergency).

IV. Conclusion

Thank you again for allowing us the opportunity to respond to these important questions. We would be happy to provide additional information or to answer any additional questions you may have.

Sincerely,

ELECTRONIC FRONTIER FOUNDATION

CINDY A. COHN