Matter of 381 Search Warrants Directed to Facebook, Inc. (New York County Dist. Attorney's Off.)
2015 NY Slip Op 06201 [132 AD3d 11]
July 21, 2015
Renwick, J.
Appellate Division, First Department
Published by New York State Law Reporting Bureau pursuant to Judiciary Law § 431.
As corrected through Wednesday, November 4, 2015

[*1]

In the Matter of 381 Search Warrants Directed to Facebook, Inc., Appellant. New York County District Attorney's Office, Respondent.

First Department, July 21, 2015

APPEARANCES OF COUNSEL

Gibson, Dunn & Crutcher LLP, Washington, DC (*Thomas H. Dupree* of the bar of the District of Columbia admitted pro hac vice of counsel), and *Gibson, Dunn & Crutcher LLP*, New York City (*Orin Snyder*, *Alexander H. Southwell* and *Jane Kim* of counsel), for appellant.

Cyrus R. Vance, Jr., *District Attorney's Office*, New York City (*Benjamin E. Rosenberg* and *Bryan Serino* of counsel), for respondent.

New York Civil Liberties Union Foundation, New York City (*Jordan Wells*, *Mariko Hirose* and *Arthur Eisenberg* of counsel), for New York Civil Liberties Union, amicus curiae.

American Civil Liberties Union Foundation, New York City (*Alex Abdo* of counsel), for American Civil Liberties Union, amicus curiae.

Perkins Coie LLP, New York City (*Jeffrey D. Vanacore* of counsel), for Dropbox Inc., and Others amici curiae.

Holwell, Shuster & Goldberg LLP, New York City (*Richard J. Holwell*, *John M. DiMatteo* and *Daniel M. Sullivan* of counsel), for Foursquare Labs, Inc., and Others amici

curiae.

{**132 AD3d at 13} OPINION OF THE COURT

Renwick, J.

This appeal raises the question of whether an online social networking service, the ubiquitous Facebook, served with a warrant for customer accounts, can litigate prior to enforcement the constitutionality of the warrant on its customers' behalf. Rather than complying with the warrant, the online social networking service moved to quash the subpoena. The motion court summarily rejected the pre-enforcement motion, and Facebook appealed. The New York County District Attorney's Office moved to dismiss the appeal, which we denied. After argument on appeal, we now hold that Facebook cannot litigate the constitutionality of the warrant pre-enforcement on its customers' behalf.

Facebook is an online social networking service with over one billion users worldwide that allows its users to create an online presence to record all manner of life events, opinions, affiliations, and other biographical and personal data. Through Facebook's online website's [*2]security settings, users can decide, through a wide variety of options, with whom they wish to share information. Options may vary, from the user who posts information publicly for every user to view, to the user who restricts the number of users who may view his/her information. Users may comment on items posted by other users, assuming those posting the content have given the viewing user access to the material and permission to comment. Facebook also has a private messaging service that works much like an email account, or text function on a smart phone.

On July 23, 2013, on the application of the District Attorney's Office, Supreme Court issued 381 substantially identical digital search warrants for Facebook accounts. The warrants sought information in 24 separate categories, essentially comprising every posting and action the 381 users identified had taken through Facebook. The warrants were obtained in connection with a large-scale investigation into the fraudulent filing of Social Security disability claims, including claims from a group of retired police officers and firefighters suspected of having feigned mental illnesses caused by the events of September 11, 2001. The application for the warrants was supported by the 93-page affidavit of Senior Investigator Donato Siciliano.

According to the warrants, there was "reasonable cause to believe" that the property to be searched and seized constituted evidence of offenses that included grand larceny in the second degree, grand larceny in the third degree, filing of a false{**132 AD3d at 14} instrument in the first degree, and conspiracy. Each of the warrants contained a nondisclosure provision, which prevented Facebook from disclosing the warrants to the users. Upon being served with the warrants, Facebook contacted the District Attorney's Office and requested that it voluntarily withdraw them, or, alternatively, consent to vacate the nondisclosure provisions. The District Attorney's Office declined.

Before Supreme Court, Facebook moved to quash the warrants, challenging their broad scope and nondisclosure requirements. The District Attorney's Office defended the warrants as a legitimate governmental action to aid an expansive investigation. Further, the District Attorney's Office justified the confidentiality requirements as necessary to prevent potential defendants from fleeing if they learned of the investigation, destroying evidence outside Facebook's control, or tampering with potential witnesses. The District Attorney's Office also questioned Facebook's legal standing to raise constitutional concerns, contending that Facebook is simply an online repository of data and not a target of the criminal investigation.

Supreme Court denied Facebook's motion to quash and upheld the warrants as issued, requiring Facebook to comply. According to Supreme Court, Facebook could not assert the Fourth Amendment rights of its users. Facebook had to wait until the warrants were executed and the searches conducted; only then could the legality of the searches be determined. Facebook complied with the warrants, and the District Attorney's Office indicted some of the targeted people.

Facebook filed an appeal from Supreme Court's order, and the District Attorney's Office moved to dismiss the appeal. On September 25, 2014, this Court denied the motion to dismiss. This Court permitted the filing of amicus briefs by the American Civil Liberties Union and several high-profile Internet companies.[FN1] While allowing Facebook's appeal to survive, the preliminary ruling was without prejudice to the District Attorney's Office's right to reassert challenges to Facebook's "right" to move to quash the warrant pre-enforcement.

[*3]

We now hold that Supreme Court's summary denial of Facebook's motion to quash the search warrants was proper because there is no constitutional or statutory right to challenge

an alleged defective warrant before it is executed. The key role of{**132 AD3d at 15} the judicial officer in issuing a search warrant is described generally by the Fourth Amendment and more specifically by state statutes. None of these sources refer to an inherent authority for a defendant or anyone else to challenge an allegedly defective warrant before it is executed.

Criminal prosecutions officially begin with an arrest. However, even before the arrest, the law protects citizens against unconstitutional police tactics. The Fourth Amendment stands as the main protector of individual privacy from government intrusion. This protection is prophylactic, as "[t]he Amendment is designed to prevent, not simply to redress, unlawful police action" (*Chimel v California*, 395 US 752, 766 n 12 [1969]). Consequently, the specific protections of the Amendment aim to deter violations from occurring in the first place (*id.*).

The U.S. Supreme Court has recognized that the Constitution, through the Fourth Amendment, provides a significant number of ex ante and ex post protections to citizens. For instance, in *United States v Grubbs*, the Supreme Court recognized that

> "[t]he Constitution protects property owners not by giving them license to engage the police in a debate over the basis for the warrant, but by interposing, *ex ante*, the *deliberate, impartial judgment of a judicial officer . . . between the citizen and the police . . .* and by providing, *ex post*, a right to suppress evidence improperly obtained and a cause of action for damages" (*United States v Grubbs*, 547 US 90, 99 [2006] [emphasis added and internal quotation marks omitted]).

The main ex ante protection derives from the Fourth Amendment's Warrants Clause, which states, "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized" (US Const 4th Amend). The Warrants Clause is the main ex ante protection because it establishes the constitutional requirements for a valid search warrant (*id.*). More specifically, under the Warrants Clause, a law enforcement official must swear, under oath, that the information contained within the search warrant is true (*id.*). Like the Fourth Amendment, article 1, § 12 of the New York State Constitution requires an oath or affirmation in support{**132 AD3d at 16} of the warrant.[FN2] Moreover, the Warrants Clause requires that the search warrant contain statements or facts that form probable cause to perform the search, as well as identify what items the police intend to seize and what places the police intend to search (*id.*). Any search warrant that does not contain the aforementioned

requirements is per se unconstitutional and may not be issued by the court or executed by the government (*see e.g. People v Gavazzi*, 20 NY3d 907 [2012]).

Whereas the Fourth Amendment provides a general framework, New York's warrant statutes explain the procedural details of who can obtain the warrant, how it can be obtained, when it can be executed, and how a return on the warrant must be filed (*see* CPL 690.45). Specifically, these statutes are designed to protect the constitutional rights of criminal suspects and defendants, beginning with the initial police investigation of a suspect. In promulgating the requirements of the warrant application, the legislature apparently wanted the judge considering the application to take nothing for granted. Accordingly, the application must include the name of the court where the application is being made, the applicant's name and title, and a request that the court issue a search warrant directing a search and seizure of the designated property or [*4]person (*see* CPL 690.35 [3] [a], [d]). The warrant application must also provide the judge with "reasonable cause" to believe that evidence of illegal activity will be present at the specific time and place of the search (*see* CPL 690.35 [3] [b]) and specify that the property sought constitutes evidence of a specific offense (*see* CPL 690.10 [4]; 690.35 [3] [b]).

Furthermore, the U.S. Supreme Court has required that a neutral and detached judicial officer or magistrate determine if a search warrant is valid under the Fourth Amendment (*see Shadwick v Tampa*, 407 US 345, 349-350 [1972]). In addition to deciding if the warrant application establishes probable cause, the neutral and detached judicial officer must also ensure the law enforcement official has sworn, under oath, that the information contained within the warrant application is true and that it identifies the places being searched and the items being seized (*see* US Const 4th Amend). In effect, the neutral and detached judicial officer serves as a constitutional gatekeeper and protects citizens from the actions of an overzealous government (*see Johnson v United States*, 333 US {**132 AD3d at 17} 10, 13-14 [1948] [noting protections of Fourth Amendment include having a neutral and detached judicial officer determine if the government has established enough probable cause to issue a search warrant]).

The motion to suppress is the most important ex post protection available to citizens. [FN3] The motion to suppress is vital, because it can lead to the suppression of unconstitutionally seized evidence. Once evidence is suppressed, the government's case could become impossible or significantly more difficult to prove. The reasons for making a motion

to suppress can be quite broad. However, in the context of search warrant cases, motions to suppress typically cover several specific areas. For instance, a motion can be made on the ground that the search warrant was not properly executed by the government (*see e.g. People v Sciacca*, 45 NY2d 122 [1978] [warrant to search a car did not authorize entry into garage, where the car was parked, to effectuate the search]). In addition, a motion can be made on the ground that the government lacked probable cause. Even though the neutral and detached judge determined that there was probable cause, the defendant has a right to have the appellate court decide whether the judicial officer's rulings were correct (*see e.g. People v Bigelow*, 66 NY2d 417 [1985]). Likewise, a motion to suppress can be made attacking the search warrant itself, if a defendant believes the search warrant is invalid on its face or does not properly describe the place being seized and the property being seized (*see e.g. People v Rainey*, 14 NY2d 35 [1964]; *People v Henley*, 135 AD2d 1136 [4th Dept 1987], *lv denied* 71 NY2d 897 [1988]).

Together, these ex ante and ex post protections typically work to successfully ensure that the government does not exceed its authority when requesting or executing a search warrant. [*5]Thus, these protections eliminate any need for a suspected citizen to make a pre-execution motion to quash a search warrant.{**132 AD3d at 18} Indeed, under New York State Criminal Procedure Law, the sole remedy for challenging the legality of a warrant is by a pretrial suppression motion which, if successful, will grant that relief. If the suppression motion is unsuccessful, and the defendant is convicted, appellate relief is limited to raising the issue upon direct appeal from the judgment. Direct appellate review of interlocutory orders issued in a criminal proceeding is not available absent statutory authority (*People v Bautista*, 7 NY3d 838 [2006]). The power of the court to authorize search warrants, generally, is set forth in CPL article 690. However, neither CPL article 690, nor CPL article 450, which sets forth when a criminal appeal can be taken, provides a mechanism for a motion to quash a search warrant, or for taking an appeal from a denial of such a motion (*see Matter of Bernstein*, 115 AD2d 359 [1st Dept 1985], *lv dismissed* 67 NY2d 852 [1986]).

Tacitly conceding that neither a defendant nor any other person has the right to move to quash an alleged defective warrant before it is executed—nor the right to appeal the denial of such a challenge—Facebook urges this Court to consider its motion to quash the search warrant as analogous to a motion to quash a subpoena, making the order denying its motion appealable. In contrast to warrants, a motion to quash a subpoena, even one issued pursuant to a criminal investigation, may be considered civil by nature, and it results in a final and

appealable order, and subject to direct appellate review (*see Matter of Abrams [John Anonymous]*, 62 NY2d 183 [1984]; *see also* CPLR 5701 [a]). The Court of Appeals reached this conclusion in *Matter of Abrams*, holding that a motion to quash a subpoena is civil in nature in that the relief sought has nothing inherently to do with criminal substantive or procedural law, and that a motion to quash can arise as easily in the context of a purely civil lawsuit as in a purely criminal case (*Abrams*, 62 NY2d at 194).

Courts, however, have imposed fairly narrow limits on the use of subpoenas for criminal discovery purposes. Although CPL 610.25 was amended in 1979 to allow the defendant (or the prosecution) to subpoena documentary and other physical evidence prior to trial (*see* L 1979, ch 413, § 3), the Court of Appeals has consistently held that a subpoena may not be used for the purposes of general discovery. Rather, the purpose of a subpoena is " 'to compel the production of specific documents that are relevant and material to facts at issue in a pending judicial proceeding' " (*Matter of Terry D.*, 81 NY2d 1042, 1044 {**132 AD3d at 19} [1993], quoting *Matter of Constantine v Leto*, 157 AD2d 376, 378 [3d Dept 1990], *affd* 77 NY2d 975 [1991]; *see also People v Gissendanner*, 48 NY2d 543, 551 [1979]).

Here, the warrants were issued prior to any pending criminal proceeding. Nevertheless, Facebook posits that what makes the warrants here more akin to a subpoena than a traditional warrant is that they were served on Facebook, which required Facebook, rather than law enforcement agents, to be responsible for "seizing" the materials by gathering the data and delivering it to the government. Even if we were to ignore the fact that the search warrants were issued prior to any pending judicial proceeding, the purported distinction, of service directly upon Facebook, is a distinction without a difference, because it simply cannot be said that quashing the warrants, the relief which Facebook seeks, "although . . . relat[ing] to a criminal matter, . . . does not affect the criminal judgment itself, but only a collateral aspect of it" (*Matter of Hynes v Karassik*, 47 NY2d at 659, 661 n 1 [1979] [order unsealing a criminal file for use in an underlying civil case was appealable as a civil order]). Thus, while, for modern technological reasons, the manner in which the materials are gathered may deviate from the traditional, Facebook's reason for seeking to quash the warrants does not. What Facebook ultimately seeks is suppression of the materials obtained from it, a determination that would necessarily impact the subsequent criminal actions.

To accept Facebook's argument is to embrace the notion that a warrant is limited only to traditional search warrants authorizing law enforcement agents to forcibly enter and search

[*6]physical places. This approach is, however, oblivious to the fact that within the context of digital information, "a search occurs when information from or about the data is exposed to possible human observation, such as when it appears on a screen, rather than when it is copied by the hard drive or processed by the computer" (Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv L Rev 531, 551 [2005]). It is also hard to imagine how a law enforcement officer could play a useful role in the Internet service provider's retrieval of the specified online information.

Alternatively, Facebook points to the Federal Stored Communications Act (SCA), which provides an Internet Service Provider (ISP) with the express right to contest any order or{**132 AD3d at 20} subpoena served upon it (*see* 18 USC § 2703 [d]).[FN4] Facebook argues that the bulk warrants in the instant case were analogous to one defined under the SCA, in that: (1) it need not be served in person (*see United States v Bach*, 310 F3d 1063, 1065 [8th Cir 2002], *cert denied* 538 US 993 [2003]); (2) it is not immediately executed (*see Hubbard v MySpace, Inc.*, 788 F Supp 2d 319, 321 [SD NY 2011]); (3) no law enforcement presence is required for service of execution pursuant to 18 USC § 2703 (g); and (4) the recipient of the SCA warrant is commanded to identify, collect, and produce information to the government (18 USC § 2703 [a]). Thus, according to Facebook, it necessarily follows that Facebook has the right to contest the warrant served upon it, as provided in 18 USC § 2703 (d). However, as fully explained below, SCA subsection (d), which gives the ISP the right to object, applies only to court orders or subpoenas issued under SCA subsections (b) or (c), disclosure devices which the SCA itself distinguishes from warrants, which are governed by its subsection (a).

Facebook's argument rests on a misinterpretation of the SCA.[FN5] The SCA is not a catch-all statute designed to protect the privacy of stored Internet communications; instead, it is narrowly tailored to provide a set of Fourth Amendment-like protections for computer communications. The Fourth Amendment to the US Constitution protects the people's right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" (*see e.g. Katz v United States*, 389 US 347 [1967]). However, when applied to information stored online, the Fourth Amendment's protections are potentially far weaker. In part, this is because computer records are stored in a technologically innovative form,[FN6] raising {**132 AD3d at 21}the [*7]question whether they are sufficiently like other records

to engender the "reasonable expectation of privacy" required for Fourth Amendment protection.

Furthermore, users generally entrust the security of online information to a third party, an ISP. In many cases, Fourth Amendment doctrine has held that, in so doing, users relinquish any expectation of privacy (*see Smith v Maryland*, 442 US 735 [1979]). The third-party doctrine holds that knowingly revealing information to a third party relinquishes Fourth Amendment protection in that information (*see* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 Michigan L Rev 561 [2009]). While a search warrant and probable cause are required to search one's home, under the third-party doctrine only a subpoena and prior notice (a much lower hurdle than probable cause) are needed to compel an ISP to disclose the contents of an email or of files stored on a server.

The SCA creates Fourth Amendment-like privacy protections for email and other digital communications stored on the Internet. It limits the ability of the federal or state government to compel an ISP to turn over content information and non-content information (*see* 18 USC § 2703). In addition, it limits the ability of commercial ISPs to reveal content information to nongovernment entities (*id*.). The basic premise of the SCA is that customers of ISPs, cell phone companies, and web-based email providers should receive statutory privacy protections for the account, transactional, and content data that these third-party providers maintain on behalf of the customer (*see* 18 USC § 2707).

Presently, the SCA authorizes three methods for obtaining information from electronic communications service providers:

1. An administrative, grand jury or trial subpoena (*see* 18 USC § 2703 [c] [2]);

2. A court order issued pursuant to 18 USC § 2703 (d); or

3. A search warrant (*see* 18 USC § 2703 [a]).

The less privacy protection afforded to the type of record, the less intrusive the legal process required. For instance, in order to obtain subscriber information, that is, the record of who subscribes to an Internet access account, including the person's name, address and credit card used to establish the account, the police need only issue a subpoena (*see* 18 USC § 2703 [c] {**132 AD3d at 22}[2]).[FN7] In order to obtain transaction data such as when an

individual accessed her account, what services she used and how long she was online, the police must obtain a court order (*see* 18 USC § 2703 [c] [1]). Similar to real time communication, in order to obtain the content of stored communications, police must obtain a search warrant (*see* 18 USC § 2703 [a], [b]).

We agree with Facebook that the bulk warrants at issue here are analogous to SCA section 2703 (a) warrants to the extent they authorized the federal and state government to procure a warrant requiring a provider of electronic communication service to disclose electronic content in the provider's electronic storage. However, contrary to Facebook's allegations, section 2703 (d), which gives the ISP the right to object, applies only to court orders or subpoenas issued under subsections (b) or (c). The SCA specifically distinguishes these disclosure devices from warrants, which are governed by its subsection (a). While an order or subpoena obtained [*8]pursuant to (b) or (c) requires only that the government show "specific and articulable facts" that there are "reasonable grounds to believe"[FN8] the information sought will be "relevant and material," a warrant under subsection (a) requires the government to make the traditional and more stringent showing of "probable cause." Here, a finding of probable cause was made by the reviewing judge, and thus the warrants are akin to SCA warrants, not SCA subpoenas or orders. Thus, Facebook's argument that it has the right to contest the warrants based upon the SCA is contradicted by the express terms of the SCA.

Facebook cannot have it both ways. On the one hand, Facebook is seeking the right to litigate pre-enforcement the constitutionality of the warrants on its customers' behalf. But neither the Constitution nor New York Criminal Procedure Law provides the targets of the warrant the right to such a pre-enforcement challenge. On the other hand, Facebook also wants the probable cause standard of warrants, while retaining the pre-execution adversary process of subpoenas. We see no basis for providing Facebook a greater right than its customers are afforded.

To be sure, we are cognizant that decisions involving the Fourth Amendment have the power to affect the everyday lives{**132 AD3d at 23} of all U.S. residents, not just criminal suspects and defendants. Our holding today does not mean that we do not appreciate Facebook's concerns about the scope of the bulk warrants issued here or about the District Attorney's alleged right to indefinitely retain the seized accounts of the uncharged Facebook users. Facebook users share more intimate personal information through their Facebook

accounts than may be revealed through rummaging about one's home. These bulk warrants demanded "all" communications in 24 broad categories from the 381 targeted accounts. Yet, of the 381 targeted Facebook user accounts only 62 were actually charged with any crime. [FN9]

Judges, as guardians of our Constitution, play an indispensable role in protecting the rights and liberties of individuals entrenched in the Constitution. Charged with the indispensable responsibility of reviewing warrant applications, they protect the rights and interests of individuals by remaining mindful of the reasonableness embedded in the Fourth Amendment's delicate balance. The procedural rules attendant to the Fourth Amendment's warrant requirement both reasonably protect the innocent and permit investigation of suspected criminal conduct. A judge reviewing a warrant request must always balance the nature and quality of the intrusion on an individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion. Further, this balance invokes carefully weighing the extent to which each level of intrusion in the execution of the warrant is needed. Each level of intrusion involves an implicit assertion by the government that the intrusion is "reasonable" to recover the evidence described in the warrant despite the compromise of the individual's interests in privacy. Ultimately, to be fair and effective, the overall assessment of reasonableness requires the judge reviewing the warrant to carefully evaluate the need for each additional level of intrusion in the process of seizing evidence.

Accordingly, the appeals from the order of the Supreme Court, New York County (Melissa C. Jackson, J.), entered on or about September 20, 2013, which denied the motion of Facebook, Inc. to quash 381 search warrants requiring Facebook to locate and produce user [*9]information, and placing Facebook under an order of nondisclosure, and from the order of the{**132 AD3d at 24} same court (Daniel P. FitzGerald, J.), entered on or about August 13, 2014, which denied Facebook's motion to compel the District Attorney's Office of the City of New York, New York County, to disclose the investigator's affidavit submitted by the District Attorney's Office in support of its application for the search warrants, should be dismissed, without costs, as taken from nonappealable orders.

Gonzalez, P.J., DeGrasse, Manzanet-Daniels and Gische, JJ., concur.

Appeals from order, Supreme Court, New York County, entered on or about September 20, 2013, and order, same court (Daniel P. FitzGerald, J.), entered on or August 13, 2014, dismissed, without costs, as taken from nonappealable orders.

Footnotes

Footnote 1: Specifically, the ruling gave technology companies Dropbox Inc., Google, Pinterest, Inc., Microsoft Corporation, Twitter, Inc., and Yelp Inc. permission to file briefs supporting Facebook's position.

Footnote 2: The wording of these rights is identical: "and no warrants shall issue, but upon probable cause, supported by oath or affirmation . . . ."

Footnote 3: Federal law, namely 42 USC § 1983, also provides a basis for litigation against local governments and local officers for constitutional violations. Section 1983 does not create any substantive rights (*see Watson v City of Kan. City, Kan.*, 857 F2d 690, 694 [10th Cir 1988] [discussing 42 USC § 1983]). Instead, it merely provides a civil remedy for the violation of a constitutional or federal statutory right (*id.*). In addition, under 42 USC § 1983, both citizens and non-citizens can file civil suits against state actors who have infringed on their federal or constitutional rights (*see e.g. Stallworth v Shuler*, 777 F2d 1431, 1435 [11th Cir 1985]). If a section 1983 claim is successful, the plaintiff could receive attorney's fees, compensatory damages, punitive damages, or even a preliminary injunction.

Footnote 4: Specifically, 18 USC § 2703 (d) states that

> "[a] court issuing an order pursuant to this section [§ 2703 (b) or (c)], 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."

Footnote 5: The Stored Communications Act, enacted in 1986, is not a stand-alone law but forms part of the Electronic Communications Privacy Act. It is codified as USC §§ 2701-2712, and addresses voluntary and compelled disclosure of stored wire and electronic communications and transaction records held by third-party Internet Service Providers (ISP).

Footnote 6: Unlike the tangible physical objects mentioned by the Fourth Amendment, computer records typically consist of ordered magnetic fields or electrical impulses (*see* Frederic J. Cooper, Computer-Security Technology 11-12 [1995]; Anthony Chandor, The Penguin Dictionary of Computers, 137-138, 255, 256, 381-385 [2d ed 1988]).

Footnote 7: The basic subscriber information listed in 18 USC § 2703 (c) (2) may also be obtained by using a section 2703 (d) order or a section 2703 (a) search warrant.

Footnote 8: This is essentially a reasonable suspicion standard.

Footnote 9:A total of 134 people were indicted in this investigation. Sixty-two of those individuals were from the 381 targeted Facebook users. Thus, 319 targeted Facebook users were not indicted.