Written Testimony of Jamil N. Jaffer[1]
before the
United States Senate
Committee on the Judiciary

on

The Electronic Communications Privacy Act:
Promoting Security and Protecting Privacy in the Digital Age

September 22, 2010

Good morning, Chairman Leahy, Ranking Member Sessions, and Members of the Committee. Thank you for the opportunity to testify today regarding the Electronic Communications Privacy Act of 1986, as amended (ECPA). I want to note, at the outset of my testimony, that the views I present today are my own and are not those of my law firm nor any client of the firm.

As the Members of this Committee are well aware, ECPA plays a crucial role in a diverse range of criminal investigations conducted by law enforcement officers from the Department of Justice (DOJ), including officers and agents from the Federal Bureau of Investigation (FBI), the Drug Enforcement Agency (DEA), and the United States Marshals Service (USMS), among others. These officers and agents work alongside other federal and state law enforcement officers and Assistant United States Attorneys (AUSAs) from across the country, as well as with prosecutors from Main Justice. These dedicated career professionals – many of whom I had the opportunity to serve with

[1] Jamil N. Jaffer is an attorney at a Washington, D.C. trial litigation firm. Mr. Jaffer previously served in the White House as an Associate Counsel to the President (2008-2009) and in the United States Department of Justice's National Security Division as Counsel to the Assistant Attorney General (2007-2008), Senior Counsel for National Security Law & Policy (2007), and in the Department of Justice's Office of Legal Policy as Counsel (2005-2006). Mr. Jaffer also served as a law clerk to Judge Edith H. Jones of the United States Court of Appeals for the Fifth Circuit (2003-2004) and Judge Neil M. Gorsuch of the United States Court of Appeals for the Tenth Circuit (2006-2007). Mr. Jaffer is a graduate of the University of Chicago Law School (J.D., *with honors*, 2003), the United States Naval War College (M.A., *with distinction*, 2006), and the University of California, Los Angeles (B.A., *cum laude*, Phi Beta Kappa, 1998).

during my time at DOJ's National Security Division (NSD) – spend countless hours working on crucial investigations to protect the safety and security of the American public.

They are assisted in this effort by tools provided by Congress, including the authorities provided in ECPA, Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended (Title III), and the Foreign Intelligence Surveillance Act of 1978, as amended (FISA), among others. In particular, the authorities provided under ECPA are often used by these career professionals to obtain and assemble the critical building blocks in cybercrime, child pornography, and national security investigations, including those related to international terrorism and espionage. In the modern era, criminals regularly use electronic devices, ranging from mobile phones to networked computers and servers to assist in their criminal enterprises, whether as the means of committing the crime itself (for example, in the transmission of digital images of minors being sexually exploited) or as a means of perpetuating the criminal activity (for example, the gang leader who keeps his hit list stored in a file on his online email account).[2]

One of the primary reasons cited in favor of substantively amending ECPA to alter the standards for the collection of certain types of communications information is the dramatic change in technology that has taken place since ECPA was first enacted. As the Members of this Committee know, ECPA was enacted in 1986 against a backdrop of emerging, innovative technologies, including electronic mail. This was, of course, well

[2] *See* United States Department of Justice, Computer Crimes and Intellectual Property Section, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE ix (3d Ed. 2009), available online at <http://www.justice.gov/criminal/cybercrime/ssmanual/ssmanual2009.pdf> (visited Sept. 18, 2010) ("CCIPS Manual").

before the development of the World Wide Web by Tim Berners-Lee at CERN in 1991, and it significantly pre-dated the massive expansion in the public use of the Internet since then, to say nothing of the concurrent evolution in the use of digital technology toward the widespread deployment and use of Internet-enabled mobile devices and "cloud computing." But simply because ECPA was first enacted long ago, in an era when the use of the Internet and networked mobile devices was dramatically less prevalent, does not mean that the principles underlying that statute and the balance that it carefully struck between the privacy interests of individuals, on one hand, and the legitimate public benefits provided by law enforcement access to certain types of communications information, on the other, is any less valid today. Indeed, what is often forgotten in the debate about ECPA is that most of the protections afforded to the public under ECPA are *not required* by the United States Constitution, including the Fourth Amendment, but rather are a matter of legislative will, enacted by Congress to protect privacy with respect to certain types of information that it believed warranted such protection.[3] As a result, while ECPA's provisions are undoubtedly complex (perhaps at times unnecessarily so), and often draw lines that at first blush may seem arbitrary, the reality is that ECPA's text and structure – including some of its most criticized provisions – are the result of nothing more and nothing less than robust debate (and ultimately a compromise) between the interests represented here today.

In striking this balance when enacting ECPA (and making subsequent amendments) – contrary to the press coverage regarding the reform proposals being

[3] As Professor Orin Kerr has noted, while the Fourth Amendment has been interpreted by the courts to provide fairly strong privacy protection for homes in the physical world, standing alone, it offers fairly weak privacy protection online. *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1211-12 (2004)

discussed today – Congress set the initial bar fairly high for broad government access to communications information. Indeed, as DOJ's Office of Legal Counsel noted in 2008, ECPA establishes a broad "background rule of privacy…generally bar[ring] a provider from giving the Government a record or other information pertaining to a subscriber or customer." *See* Requests for Information Under the Electronic Communications Privacy Act, Memorandum Opinion for the General Counsel of the Federal Bureau of Investigation (Nov. 5, 2008), available online at <http://www.justice.gov/olc/2008/fbi-ecpa-opinion.pdf> (visited on Sept. 18, 2010) (discussing the general bar on disclosure contained in 18 U.S.C. § 2702(a)). Indeed, OLC relied on this fact about ECPA in part to buttress its conclusion that the national security letter (NSL) provision of ECPA did not afford the FBI access to certain data that it sought to compel from communications providers. *Id*. (noting that the provisions of ECPA granting government access to communications records constitute specific exceptions to the broad, general rule of privacy set forth in the statute and holding that, as such, additional exceptions would not be implied). Thus, it is clear that in enacting ECPA, Congress acted to ensure that the tools available to the government in this new and emerging space were carefully regulated in order to protect the interest of individuals in the privacy of their communications while preserving the ability of the government to obtain the information necessary when appropriate.

While ECPA provides rules for government access to both content and non-content information, it makes sense to focus first on the non-content information that the government might obtain, because it is this information, in particular, that is perhaps most important to investigators in the early stages of their work. Such non-content information

is comprised of, among other things, the metadata associated with a communication, including the information use to route and transmit a communication from end-to-end, as well as the subscriber information and other records associated with a given user account or identifier. Access to communications metadata and subscriber information can help investigators determine, among other things, what email address or phone number a particular individual is using, what communications provider supports the account, as well as identifiers associated with other suspects the individual is in communication with, when such communications took place, how long the communications lasted, and various other details of the target's communications activities, other than the content itself. Such records can also provide information about the location of a given individual, both on a historical and on a going-forward basis.

Not surprisingly, such information can be crucially important to investigators at the outset of an investigation, in part, because such information serves a sifting function, permitting law enforcement to determine whether a particular individual is properly the subject of investigation and whether the use of additional techniques might be warranted, as well as providing the factual support for any such additional investigative authority the government might seek, whether through court authorization or otherwise. At the same time, of course, these building block investigative techniques – seeking non-content information in the hands of third parties – also allow the government to determine that a given individual is *not* properly the focus of an investigation, that they have no connection to the activities the government is investigating, and therefore that they can appropriately be excluded from any further investigation. Such information thus can serve a privacy enhancing function, by ensuring that a given individual is only subject to

the minimal investigative techniques necessary. Thus, the tools provided in ECPA and other statutes permitting the government to obtain non-content communications information in the hands of third parties serves both law enforcement and privacy interests, conserving limited investigative resources and helping ensure that the government conducts only the minimum intrusion necessary into an individual's communications activities at the outset of an investigation.

And ECPA already limits the way in which the government may obtain these crucial investigative building blocks, by permitting particular types of data to be obtained only in certain circumstances and then only through certain processes, with a sliding scale of increasing authorizations and predication for more invasive techniques. Indeed, it is critical to note here that in creating a general bar prohibiting government access to certain non-content communications information in the hands of third-parties and providing a specific set of exceptions to this general bar in ECPA, Congress effectively limited the government's ability to obtain information that it would typically obtain, in other contexts, through a subpoena. Indeed, the background rule generally applicable here, is that an individual typically does not retain an objectively reasonable expectation of privacy in information voluntarily conveyed to a third party, even when is conveyed with the expectation that it will remain confidential. *See, e.g.*, *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979) ("[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."); *see also, e.g.*, *SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984) ("[W]hen a person communicates to a third party even on the understanding that the communication is confidential, he cannot object if the third party conveys that information or records thereof to law enforcement authorities."); *United*

States v. Miller, 425 U.S. 435, 443 (1976) ("The Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."). And, while there are a number of important exceptions to this general background rule, including those potentially applicable to the content of communications, for example, while they are in transit, *see, e.g., United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004) (analogizing the expectation of privacy of in the contents of email to that in letters transmitted via regular mail), most of these exceptions do not apply to the non-content information that forms the critical building blocks of an investigation and which may be obtained, under certain circumstances, with less than a warrant under ECPA, *see Smith*, 442 U.S. 744-45 (holding that telephone customers have no legitimate expectation of privacy in dialing, routing, addressing, and signaling information transmitted to telephone companies); *United States v. Forrester*, 512 F.3d 500, 510-11 (9th Cir. 2008) (no reasonable expectation of privacy in information used to transmit Internet communications to and from users); *see also, e.g., United States v. Perrine*, 518 F.3d 1196, 1204 (10th Cir. 2008) ("Every federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation."); *Guest v. Leis*, 255 F.3d 325, 356 (6th Cir. 2001).

Of course, the non-content data held by communications service providers comes in different varieties, and it is not unreasonable to argue that Congress ought provide stronger statutory protection for certain kinds of information versus others. For example, one might think that subscriber records ought generally be accessible to law enforcement

through, among other things, an administrative subpoena or a subpoena issued in the course of a grand jury investigation. *See, e.g.*, 18 U.S.C. § 2703(c)(2). At the same time, one might think that transactional records or account logs ought generally be accessible to the government not simply with a subpoena, but typically with some measure of direct judicial supervision, albeit perhaps on a showing less than probable cause. *See, e.g.*, 18 U.S.C. § 2703(c)(1)(B).[4] Of course, as the preceding citations demonstrate, ECPA make just such distinctions, generally requiring providers to disclose such non-content data to the government only under particular circumstances and, where appropriate, with judicial oversight.

And it is no different with content. ECPA already places stringent restrictions on government access to data stored by third parties on behalf of their customers. *See, e.g.*, 18 U.S.C. § 2703(a)-(b). Now, it is true that many of the rules applicable to stored communications seem archaic and appear to be a product of an era when the Internet involved the use of dial-up connections, where communications were only stored for short periods of time on servers maintained by internet service providers (ISPs), and where cloud computing was not the norm. For example, critics have pointed to the statutory rule in ECPA that treats stored communications differently depending on the length of time they are stored by a particular type of provider. *See* 18 U.S.C. 2703(a). Similarly, critics have also pointed to the fact that the Department of Justice has (often successfully) taken the position that a warrant is not required to obtain the content of communications stored by a third party once the communications have been retrieved by the putative recipient, even if they have been in storage only for a short period of time.

[4] Of course, ECPA also permits law enforcement access to such data without a court order under other circumstances, such as with the consent of the customer or subscriber, *see* 18 U.S.C. § 2703(c)(1)(C).

See CCIPS Manual at 129 (noting that in jurisdictions other than the Ninth Circuit, as a general matter, "[a]gents…can [] obtain [opened and sent] email…using a subpoena.").

The very fact that ECPA draws certain lines with respect to certain types of communications information based, in part, on the type of third-party entity stores them, how long they are held by the third party, and the like, reflects a measured legislative judgment of the appropriate balance between privacy and security. This is not to suggest that this legislative judgment cannot be revisited; it certainly can, and perhaps, as discussed below, should be revisited in certain areas. However, what it is important to note is that the lines drawn in ECPA are less the result of technological developments that the law has failed to keep up with, and are more the result of compromises made in the legislative process regarding where the appropriate lines ought to be. As such, it is important that any major change in the level of authorization required for government access to certain types of communications information or in the type of showing the government must make, ought carefully be considered, and always with an eye towards balancing individual privacy and law enforcement interests.

Indeed, the notion that ECPA is stuck in the past and can't adequately deal with or account for modern technology is simply a canard. In point of fact, ECPA has been amended more than dozen times since its enactment in 1986, including as recently as last year. These amendments, which have varied from the substantive to the technical, have consistently sought to balance the interests of law enforcement with Congress's legitimate desire to protect the personal privacy interests of Americans. At the same time, the government's use of ECPA has kept pace with developments in technology, as the government now regularly uses ECPA to obtain categories of information that hardly

even existed when ECPA was first enacted in 1986, including, for example, cell-site locational information. These facts reflect the continued vitality of this statute in the modern technological environment. And while some have argued that ECPA does not account for the development of the new cloud computing environment, the fact is that cloud computing as it is currently conceptualized is somewhat analogous to what ECPA refers to as remote computing services, where service providers host customer data and run the primary applications on their own servers, rather than the customer running the applications locally. While advocates of cloud computing may reasonably be concerned that the protections provided to customer data stored with a provider of remote computing services are not commensurate with their understanding of the appropriate level of privacy due to their customers' files (and perhaps may not even be commensurate the customer's own views as to the appropriate level of privacy for his or her files), this is less a product of the change in technology and perhaps more a reflection of a change in public perceptions about where the balance between privacy and security ought be struck.

Another canard present in the ongoing public debate is that law enforcement is run amok in the cyber realm, collecting reams upon reams of data about ordinary Americans. The fact of the matter is that there is little, if any, data to support the claim that there have been extensive abuses of the authority granted law enforcement under any of the provisions of ECPA that are under discussion today. To the contrary, at a time when the Justice Department's Inspector General has taken a close look at many of the statutory tools provided to law enforcement and intelligence officers, including the authorities provided under FISA and the USA PATRIOT Act, the DOJ IG has put forward no report that I am aware of indicating a broad-based abuse of any of the ECPA

authorities that are the subject of the existing reform proposals. And, moreover, where concerns have arisen – for example, with respect to national security letters (including those issued under ECPA) – DOJ has moved swiftly to implement substantive reforms. Having served as part of the initial effort organized by the Office of the Attorney General and the National Security Division to respond to the concerns raised by the IG's first report on NSLs, I can attest to the utter seriousness with which the Department's senior leadership tackled these issues and the aggressiveness with which the Department implemented broad, sweeping reforms, including the creation of an unit within NSD's Office of Intelligence dedicated solely to oversight, and the institution of regular, consistent reviews of the FBI's use of national security investigative tools, even beyond NSLs.

All of this is not to say that some measure of ECPA reform is unwarranted, or that Congress should simply let the matter drop. To the contrary, I think there is substantial room for improvement in the existing statute and I firmly sympathize with the complaints from industry and others regarding the statutory ambiguities that exist in ECPA, as well as the often confusing (indeed, bewildering) array of standards, authorities, and definitions set forth in the statute, to say nothing of the diversity of the judicial decisions interpreting ECPA and the background constitutional rules. To pick just one example of many, one need only look to the Third Circuit's decision issued earlier this month, where that court held ECPA provides magistrate judges with the discretion to require the government to meet a higher standard (and even perhaps to obtain a warrant) in order to obtain information – in that case, historical cell site data – that the court determined would otherwise be available (without a warrant) under ECPA's court order provision.

See In the Matter of the Application of the United States of America for an Order Directing a Provider of Electronic Communications Service to Disclose Records to the Government, __ F. 3d __, slip op. at 21-29 (3d Cir. Sept. 7, 2010). This decision, standing on its own – not to mention the multitude of opinions across the country regarding the standards the government must meet in order to obtain historical or prospective cell site data – demonstrates that there is, in fact, a need for a close look at ECPA and that there may be room for some useful clarification of the existing statutory language.

At the same time, it is hard to understate the importance of ensuring that law enforcement has consistent, ready access to much (if not more) of the communications information that it has today. This is so because we live in an era of increasing, not decreasing cyber threats, ranging from transnational criminal gangs, to hackers, to national security threat actors, including hostile governments and increasingly sophisticated terrorist groups. Moreover, government access to communications information is perhaps most critical in protecting the most vulnerable amongst us: our children. There is a growing body of anecdotal evidence from investigators (and some literature) to support the notion that pedophiles find substantive encouragement of their activities in online communities, and that this encouragement often results in increasing rates of illegal image sharing, as well as in these individuals taking further illegal action in the real world. These fora also often provide information on how these criminals might best hide their tracks on the Internet, directing them to providers and resources that make law enforcement's efforts to protect our children that much more difficult. In this way, child predators are much like potential terrorists online, finding encouragement,

support, and training over the Internet. Indeed, in many ways, these communities on the Internet can serve as a network of virtual caves and hideouts for child pornographers, cybercriminals, and foreign operatives alike, much like the Tora Bora complex in Afghanistan or the terrorist safe houses that dot the landscape of the Northern Areas of Pakistan. To limit the ability of our law enforcement personnel to ferret out these virtual hideouts and to track down their inhabitants in an era when the threat is growing and is more imminent raises obvious concerns. Indeed, in the absence of any substantive evidence of abuse or misuse of these authorities by law enforcement personnel, one may reasonably question the wisdom of substantially limiting (and essentially disarming) our frontline personnel in the fight against these cyber predators.

My strong recommendation, as a result, is that Congress proceed quite cautiously and with deliberation in considering amendments to ECPA. Substantive changes to the statutory standards for accessing communications information covered by ECPA could have a dramatic and detrimental impact on law enforcement and the public safety. Thus, I recommend a three-step process for Congress's consideration of ECPA reform:

First, in my view, there are a number of somewhat modest amendments that Congress can make now to ECPA that would usefully clarify the statute, make it easier for industry to comply, and address existing issues created by outlier judicial decisions. For example, Congress could consider how to harmonize the existing definitions describing providers under ECPA, which currently make little sense, given that they differentiate between services that have largely merged in recent years, with communications services providers often providing both electronic communications services and remote computing services in the course of a given communications event.

See, e.g., CCIPS Manual at 117-20, 125-26. Similarly, Congress could likely easily address statutory ambiguities, like those that led to the Third Circuit decision described above, as well as the Ninth Circuit's outlier opinion in *Theofel v. Farey-Jones*, 359 F.3d 1006 (9th Cir. 2004), regarding the definition of electronic storage. These changes can likely be made through a consensus process and can almost certainly be completed in the next session of Congress.

Second, Congress should hold hearings over the next few months, and perhaps into the next session, specifically focused on each authority that it is considering substantively modifying. These hearings should focus on four issues with respect to each such authority: (1) how the government uses the current authority provided by statute and the tangible benefits to the public of the use of such authority; (2) whether the public's objectively reasonable expectation of privacy in the information sought by the government has substantively changed since the authority was provided; (3) whether there is any tangible, clear evidence of abuse or misuse of the authority by the government and whether such abuse, if any, is the result of procedures and processes that might be addressed through internal controls and reforms, rather than through legislative changes that would make the authority harder to obtain or use; and (4) the impact of any substantive change on the ability of law enforcement to protect the public.

Third, having determined what authorities ought be changed based on a careful balancing of the various interests at stake, Congress ought further consider whether additional provisions are necessary to counterbalance the impact of any such changes on public safety. So, for example, if Congress determines that it is in the public interest to raise the statutory standard for obtaining certain types of information from say a

subpoena to a court order, or from a court order to say a warrant, Congress may also consider requiring communications service providers to retain the covered information for longer periods of time. Such a provision could serve to ameliorate the additional burdens placed upon the government, including but not limited to the inevitable delays associated with a more onerous (but rigorous) authorization process.[5]

In sum, the message I hope to have conveyed today is as follows: (1) ECPA plays an important role in today's increasingly cyber-connected world, both in terms of protecting individual privacy interests, as well as ensuring public safety by providing government access to certain types of communications information in the hands of third-party service providers; (2) ECPA can (and should) be improved and made more consistent and clearer, particularly with an eye towards making the compliance process less onerous on providers; (3) any substantive changes to the authorization or predication levels contained in ECPA should be approached with great caution and a due regard for the implications of such changes on law enforcement investigations; and (4) where appropriate, Congress ought consider offsetting any substantive changes made to the authorities contained in ECPA by ensuring that the government has access to the relevant data once the appropriate requirements are met.

Thank you very much for the opportunity to present my views today.

[5] As the Committee may be aware, the Department of Justice has long considered the issue of data retention and, having served as the coordinator of one such working group led by the Assistant Attorney General for Legal Policy back in 2006, I can attest to the value of such a provision for the government's law enforcement efforts, in particular in child exploitation investigations. Of course, there are significant issues that would need to be addressed including cost and liability issues for industry, as well as the privacy and security implications of large amounts of data being retained by providers.