No. 03-1383

UNITED STATES COURT OF APPEALS
FOR THE FIRST CIRCUIT

UNITED STATES OF AMERICA,
Appellant
v.

BRADFORD C. COUNCILMAN
Defendant-Appellee

On Appeal From A Judgment In A Criminal Case
Entered In The
United States District Court
for the District of Massachusetts

BRIEF FOR THE DEFENDANT-APPELLEE

Respectfully submitted,

BRADFORD C. COUNCILMAN

By his attorney:

ANDREW GOOD
Good & Cormier
83 Atlantic Avenue
Boston, MA 02110
(617) 523-5933

TABLE OF CONTENTS

TABLE OF AUTHORITIES

FEDERAL CASES

FEDERAL STATUTES

LEGISLATIVE REPORTS

MISCELLANEOUS

STATEMENT OF JURISDICTION

Bradford Councilman ("Councilman") adopts the government brief's statement.

STATEMENT OF ISSUES

Whether an employee of an electronic communication service who obtained the contents of electronic communications on an ongoing, real-time basis, while the communications were in electronic storage in the computer facilities of that service, acted lawfully under 18 U.S.C. § 2701(c)(1), or illegally intercepted the communications in violation of § 2511(1)(a).[1]

STATEMENT OF THE CASE

Councilman adopts the government brief's statement with the following additions and clarifications. In its Memorandum and Order dismissing the count, the district court refers to motions *in limine* concerning the defense's expert testimony and certain prosecution evidence as well as requests for jury instructions, all of which were under advisement at the time that it reconsidered its initial ruling denying the motion to dismiss. *United States v. Councilman*, 245 F. Supp. 2d 319, 320 (D.Mass. 2003). In order to understand the effect these litigation events had on the district court's ruling, this Court should review the proposed expert testimony, motions *in limine*,

[1] All statutory citations are to sections of Title 18, United States Code, unless otherwise indicated.

and jury instruction requests. For example, the district court was referring to the motions *in limine* and requests for jury instructions when it stated: "Sorting out what forms of 'storage' are covered by the statute may prove an evidentiary nightmare at trial and pose a challenge for proper jury instructions." *Id*.

Summaries of Expert Opinions

On November 15, 2001, the government filed its summary of expert testimony. J.App. 73-76. The summary describes what it referred to as "typical" electronic mail processing. However, the government's summary indicated that its proposed expert had neither examined the data seized during an FBI search of Interloc's computers, nor did the expert summarize any opinion about the characteristics and operation of the specific mail processing system at issue: Interloc's. In particular, the proffered opinion did not address whether the electronic communications at issue were in electronic storage within the computer facilities Interloc used to provide its electronic communication service, when Interloc's procmail script made copies of some of them.

On March 8, 2002, Councilman filed his summary of expert testimony, reporting on the experts' examination of the FBI-seized data, opining that Interloc's procmail script made copies of certain electronic

communications while the communications were electronically stored within Interloc's electronic service provider facilities, and providing detailed reasons for these assertions. J.App.81-92. After the parties' exchange of summaries of expert summaries, the defendant's motion to dismiss was filed on April 16, 2002 (D.26), which relied partly on a stipulation. J.App. 23.

Jury Instruction Requests

After the district court's July 11, 2002 initial denial of the motion to dismiss, J.App.65-67; 72, the government submitted requests for jury instructions concerning the interception offense. J.App. 126. The prosecution request would not have required the government to prove that the electronic communications in question were not in electronic storage within the facilities of Interloc's electronic communication service, when copies of them were made by Interloc. J.App.131-133. Councilman's request required the government to prove that the electronic communications in question were not acquired by the alleged conspirators while they were in electronic storage in Interloc's facilities, J.App. 145-148. His requests also required the government to prove that Councilman did not rely in good faith on § 2701(c)(1)'s statutory authorization that permits employees of an electronic communication service to lawfully obtain access to electronic

communications while they were in electronic storage in the service's facilities. 18 U.S.C. § 2520(d)(1). J.App.149.

The Parties' *In Limine* Motions

When the government filed its requests for jury instructions, it also moved *in limine* to exclude entirely the proposed testimony of Councilman's experts, to exclude the defense's evidence of the custom or practice of electronic communication service providers to engage in activities that were electronically identical to Interloc's activities, and to prevent Councilman from asserting a good faith defense based on §§ 2520(d)(1) and 2701(c)(1). D.47. Councilman likewise moved *in limine* (D.48) to exclude evidence of Interloc's acquisition of certain electronic communications while they were stored at locations in Interloc's computers identified as the addressees' in-boxes (*see e.g.* J.App.135-40), or stored for backup protection purposes (*see e.g*. J.App.143), in part, because these activities were lawful under § 2701(c)(1). The parties filed oppositions to each other's *in limine* motion. D.49&51.

The Hearing Concerning *In Limine* Motions and Jury Instructions

On November 25, 2002, the court heard argument on the parties' *in limine* motions and their requests for jury instructions under advisement after a hearing on that day. *See* Supplemental Appendix ("Supp.App."). At

the hearing, the central issue was whether the district court would permit the parties to litigate before the jury what the court referred to as "the 2701 defense": whether the electronic communications were acquired by Interloc while they were in electronic storage in its computer facilities as described in §§ 2510(17) and 2701(c)(1), or whether evidence and jury instructions pertaining to those provisions would be excluded from the trial.

Before ruling on the motions and requests, the court issued its December 2, 2002 order requesting that the parties brief whether denial of the motion to dismiss should be reconsidered in light of *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002), *cert. denied*, 123 S. Ct. 1292 (2003) and particularly footnote 6. J.App. 172-178. Prior to the December 2 order, neither party had been aware of the 9th Circuit's opinion after rehearing in *Konop*. After considering the parties' post-*Konop* submissions (D.56-61), the Court dismissed the count and this appeal ensued.

STATEMENT OF FACTS

Section 1 of the government's statement is not about facts; it is a legal argument about the Electronic Communications Privacy Act ("ECPA") which will be addressed in the argument section of this brief. Section 2 describes the allegations of the indictment and the grounds asserted in the

motion for its dismissal somewhat misleadingly. The parties stipulated to facts that apply at all times material to the motion to dismiss.

1. Each of the electronic mail messages at issue was an "electronic communication" within the meaning of § 2510 (12). J. App.26 (¶7). When processing the electronic communications at issue, Interloc acted as an electronic communication service within the meaning of § 2510 (15), and Councilman acted as an Interloc vice-president, shareholder and employee. J.App.24 (¶¶ 1&2).

2. Electronic mail is the transfer of electronic communications in *store and forward* fashion from computer to computer through a network of telecommunication cables. J.App.24-25 (¶3).

3. Interloc's computer facility used a computer program called procmail (for "process mail") as its message delivery agent ("MDA"). Procmail operated by scanning and sorting mail after it had been processed by an MTA computer program known as sendmail. In January 1998, Interloc's systems administrator wrote a revision to procmail, known as procmail.rc, which copied on an on-going and prospective basis, all incoming messages from Amazon.com. J.App.26 (¶ 4).

4. The Mail Transfer Agent ("MTA") sendmail and the MDA procmail operated exclusively within Interloc's computer. At all times that

sendmail and procmail performed operations affecting the email messages at issue, the messages existed in the random access memory (RAM) or in hard disks, or both, within Interloc's computer system.[2] J.App.26 (¶ 5).

5. Neither sendmail nor procmail performed functions that affected the emails in issue while the emails were in transmission through wires or cables between computers. J.App.26 (¶ 6).

Relying upon these stipulated facts, the district court found and ruled as follows:

> The definition of "electronic storage" is extraordinarily -- indeed, almost breathtakingly -- broad. See *18 U.S.C. § 2510* (17). It covers "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof," as well as "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." (Emphasis supplied).

---

[2] All storage components within each computer fall into one of two categories: primary storage and secondary storage. A computer's primary storage is "[t]he computer's main memory, which consists of the random access memory (RAM) and the read-only memory (ROM) that is directly accessible to the central processing unit (CPU)." Bryan Pfaffenberger, Webster's New World Computer Dictionary, 296 (9th ed. 2001). Each computer stores email in its RAM while processing it. See Id. at 309 (Defining RAM as "[t]he computer's primary working memory, in which program instruction and data are stored…,"). Secondary storage, in contrast, is "[a] nonvolatile storage medium, such as a disk drive, that stores program instructions and data even after one switches off the power." Id. at 328. Although all computers used to provide electronic communication service, such as Interloc's, must keep a copy of an email message in primary storage (the RAM) so that it can be processed, most, including Interloc's computer, also copy each email into a queue for backup protection purposes in a form of secondary storage (like a hard drive) through the use of email processing program called Sendmail.

> Given this definition, there can be no serious question that the communications underlying the indictment in this case were "in storage" at the time the defendant is alleged to have intercepted them. As the stipulation entered into by defendant and the Government indicates, they were "in the random access memory (RAM) or in the hard disks, or both, within Interloc's computer system" at the time of the supposed interception. Stipulation at ¶ 5.

United States v. Councilman, 245 F. Supp.2d 319, 320-321 (D.Mass. 2003) (emphasis supplied).

The stipulated location of the electronic communications in the random access memory (RAM), or in the hard disks, or both, within Interloc's computer system at the time Interloc made its copies of the Amazon-sourced messages, incontrovertibly establishes that the electronic communications were at the material times in electronic storage. Even though the district court's ruling explicitly rests on the "extraordinarily" broad definition of "electronic storage" § 2510 (17), the government's brief does not even attempt to explain why the text of this provision does not apply in this case. The Senate Judiciary Committee report on the ECPA carefully explained the intended scope of each of §2510's definitions. On the subject of the "electronic storage," the Judiciary Committee wrote:

> The term 'electronic storage' is defined in proposed subsection 2510(7) [sic] of title 18. Electronic storage means (A) the temporary, intermediate storage of a wire or electronic communication incidental to its transmission as well as (B) the storage of such communication by an electronic communications service for backup protection. *The term covers*

> *storage within the random access memory of a computer as well as storage in <u>any</u> other form including storage of magnetic tapes, disks or other media.*

S. Rep. 99-541 at 16 (1986), reprinted in 1986 U.S.C.C.A.N. at 3570 (emphasis supplied).

Tellingly, though Councilman's district court briefs featured the Senate Report's clarification of "electronic storage," and the district court clearly relied on it, the government's brief ignores it.

Instead, the government's brief obfuscates the facts by attempting to analogize Interloc's procmail script to a "siphon." The government does not dispute that, in fact, all that the procmail script did was automatically make extra <u>copies</u> for Interloc's use of Amazon-sourced emails addressed to Interloc's subscribers. The district court agreed that what occurred within Interloc's computers was not "transmission" of messages, as the government would have it, but rather <u>copying</u> of them. Supp. App.21. Nor does the government dispute either the factual or the legal correctness of the district court's ruling that this extra <u>copying</u> occurred while the electronic communications were in § 2510(17) electronic storage in computer facilities Interloc used to provide electronic communication service to its book dealer-subscribers.

Specifically, the government's brief does not assert that the stipulated facts relied upon by the district court are either insufficient or immaterial as support for its legal conclusion that Interloc's procmail script copied the electronic communications "while in electronic storage" within the meanings of §§ 2701(c)(1) and 2510(17).

Arguments of counsel during the November 25, 2002 hearing concerning the parties' *in limine* motions and requests for jury instructions presaged the dismissal of the count. Defense counsel illustrated Councilman's § 2701 defense by pointing out that, prior to the alleged conspiracy period and by electronic means different from the procmail script, Interloc obtained access to electronic communications addressed by others to Interloc subscribers by making copies of the communications from Interloc's "dead letter" file. The copies in the dead letter file existed for backup protection purposes. Counsel pointed out that Interloc had also obtained copies of those messages, not merely "while in electronic storage," but literally by making copies from the copies (copying the copies) that existed in Interloc's backup protection file. J.App.143. Supp. App. 10-12. Likewise, defense counsel pointed out that, before the alleged conspiracy period, Interloc made copies of other messages, not merely "while" in "temporary, intermediate storage incidental to transmission," but by making

copies from the copies (copying the copies) stored in areas within Interloc's disk drive designated as the addressees' electronic mailboxes. J.App. 23, 135-139. In support of his request for jury instructions and in opposition to the government motion to exclude the testimony of Councilman's experts, defense counsel argued that the government conceded that "email read in the user's mailbox is covered by the Stored Electronic Communications Act." Supp. App. 31. Defense counsel argued that, in light of this concession, the government bore the burden to prove that, unlike the copying illustrated by the sample messages attached to the motion *in limine*, the allegedly intercepted messages were neither in Interloc's backup protection file, nor in the addressees' mailboxes, at the times that Interloc obtained access to them. Defense counsel also argued that Councilman was entitled to present expert testimony to prove that messages were copied by Interloc's procmail script while the messages were stored for backup protection or in the user's mailboxes, or both, and hence the copying was lawful under § 2701(c)(1).

The government denied that its concession meant that it would have to prove that messages were not copied by Interloc's procmail script "while in electronic storage." The government urged the court to reject the defense's requested jury instructions to that effect, and to exclude Councilman's proposed expert witnesses.

> I submit, Your Honor, all we need is the procmail script. We need the witnesses to say that Mr. Councilman instructed them to do this. *How the procmail script worked, where the copy is made in the flow*, and then the Court will instruct that an interception is the use of a device, including an electronic device, to intercept -- to intercept or copy a communication while the transmission and contemporaneous with that transmission. That's what the cases say. That's what the cases say. It's really very simple.
>
> What Mr. Good would like to do is to muck it up tremendously with reference to the Stored Communications Act which is irrelevant, and if the Court reads it, what it does is it limits access to stored communications. It doesn't authorize it.

Supp. App. 36 (emphasis supplied). Hence, the government argued untenably that: (1) its stipulation that all of copying operations performed by the procmail script while the affected messages were in Interloc's "RAM, or on its hard drive, or both" is irrelevant in determining whether § 2701 applies to the activity in question; and (2) the prosecution, but not the defense, should be allowed to present evidence as to "how the procmail script worked," and "where the copy is made in the flow." After considering the clearly correct understanding of the ECPA explained in the *Konop* opinion, and having in mind the ways in which the parties' motions *in limine* and requests of jury instructions highlighted the flawed reasoning underlying the count, the district court dismissed it.

Rather than confront the "electronic storage" facts forthrightly, the government's fact statement focuses on the sequence of electronic processing steps or events effectuated by Interloc's procmail software. The

government does not say why or how the order of electronic events provides the slightest factual basis to doubt that the entire sequence – whatever it was – occurred "while the electronic communications were in 'electronic storage,'" in the computer facilities of Interloc, an electronic communication service, as described in §§ 2701 and 2510(17).

Paragraph 12 of the indictment alleges that "The procmail.rc script worked to intercept incoming electronic mail messages before they were delivered to the intended recipient's electronic mailbox and before the message was read by the intended recipient." J.App.17 (emphasis supplied). For purposes of this motion to dismiss, Councilman agrees that the facts alleged in the indictment as well as stipulated facts -- but not legal characterizations of the facts such as the word "intercept" -- are to be taken as true. Accordingly, Councilman contends for reasons stated in the district court's opinion and in this brief that, even if Interloc's procmail script obtained access to and acquired "the incoming electronic messages before they were delivered to the intended recipient's electronic mailbox and before the message was read by the intended recipient," all of these events occurred while the electronic communications were in electronic storage in Interloc's facilities as described in §§ 2701 and 2510(17). Hence, no interception occurred.

By accepting the allegations of the indictment concerning the sequence of electronic events to be true solely for purposes of the motion to dismiss, Councilman is in no way conceding in the event of a remand for trial, that the electronic sequence of events occurred as described in the indictment. The defense experts' examination of Interloc computer data seized by the FBI showed that Interloc's mail processing software, called Sendmail and Procmail, included a feature called "SuperSafe", which entailed storage in a "queue" of copies of all incoming messages for backup protection purposes. This § 2510(17)(B) backup storage lasted until all other mail processing functions for each message were completed, at which time a signal would cause the backup copy to be deleted from Sendmail's SuperSafe queue. J.App.84-85 ¶2(f)&(g). With respect to § 2510(17)(A) storage, the defense expert summary states:

> With respect to the mail messages sent from the internet domain amazon.com, *procmail* (as instructed by the *procmail* script) copied each electronic mail message received on its input via a Unix pipe from one area of storage (the *sendmail* queue) to two other areas of storage: (1) The *procmail* program appended each such electronic mail message to the file constituting the addressee's mailbox; and (2) The *procmail* program appended each such electronic mail message to a file called *nile*. During this entire copying process, the electronic mail messages were in storage, and were also in the *sendmail* queue on the Interloc computer's hard drive. At no time during the entire copying operation were the electronic mail messages not in storage.

J.App.85 ¶2(i). The defense pointed out that nothing in the government's summary of expert testimony reflects any examination of the particular mail processing system in use at Interloc, much less rebuts the electronic sequence of events described by Councilman's experts. D.27 at 15-16. Even in the face of this challenge, the government never submitted any supplemental expert summary contradicting the defense's description of the sequence of electronic events effectuated by the sendmail and procmail script software used by Interloc.

In view of the stipulated facts concerning the locus of the electronic events in Interloc's RAM or hard disk or both, and the whole record, the district court's opinion correctly states: "Given this definition, there can be no serious question that the communications underlying the indictment in this case were "in storage" at the time the defendant is alleged to have intercepted them." *Ibid.*

SUMMARY OF ARGUMENT

The ECPA provides a simple rule that requires affirmance of the charge's dismissal. If the communication is in a wire between computers, it can be intercepted. If the communication is in an electronic communication service provider's computer, its content can be acquired lawfully by that provider's employees.

The ECPA divides and regulates the privacy of an electronic communication, depending, at any given moment, on whether it is evanescent and in transmission from computer to computer through telecommunication cable (Title I's Wiretap Act), or while it is in "electronic storage" in computer facilities of an electronic communication service (Title II's Stored Communications Act). The ECPA classifies electronic mail as entitled to less privacy protection while it is in "electronic storage" in computer facilities of an "electronic communication service," because users of electronic mail are deemed to understand that their electronic messages must be stored, and that access to their content may be obtained, by electronic communication service providers.

The district court's ruling correctly applies § 2701(c)(1), which states that Councilman's "access" to a "facility through which an electronic communication service is provided," was authorized by that service, Interloc, and that he "thereby obtain[ed]…access to an electronic communication "while it is in electronic storage in such system" lawfully. *Id*. (emphasis supplied). Section 2711(1) states that the specialized meanings of "electronic communication," "electronic communication service" and "electronic storage," when used in § 2701, are supplied by § 2510 (12), (15) and (17), respectively. The court's ruling correctly

understands and applies the meanings of all of these provisions, particularly both subsections of § 2510(17) "electronic storage": "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication."

Nothing in the government's brief shows that the district court misunderstood or misapplied the relevant statutory text, §§ 2701(c)(1) and 2510(17). Nor does it claim, much less demonstrate, that the stipulated facts are deficient to establish that Councilman's conduct was lawful under § 2701(c)(1). All the words in these two provisions perfectly fit and describe what occurred here, according to the stipulated facts.

Indeed, in prior cases, the government has taken exactly the opposite position from that urged here. In the *Konop* and *Steve Jackson* Games cases, the government successfully urged the 9th and 5th Circuits that communications cannot be intercepted while in electronic storage in computer facilities of an electronic communication service, but may be intercepted only when in transmission from computer to computer, through telecommunications cables. Due process principles estop the government from arguing otherwise to prosecute Councilman.

There is no support in ECPA text or applicable precedents for the application of the non-statutory phrases – "contemporaneous with transmission" and "static acquisition" – that the government uses in its attempt to criminalize conduct declared lawful by § 2701. The 9th Circuit has rejected the government's interpretation in *Konop v. Hawaiian Airlines, Inc.,* 302 F.3d 868, 879 n.6 (9th Cir. 2002). The government's heavy reliance on *In re Pharmatrak*, 329 F.3d 9, 21-22 (1st Cir. 2003) and *United States v. Steiger*, 318 F.3d 1039, 1046 (11th Cir. 2003), is misplaced, because none of the computers involved in effectuating the interception at issue in those cases was a § 2701 "facility through which an electronic communication service is provided." In both of these inapposite cases, claims that § 2701 applied were explicitly rejected based on the absence of outcome-determinative facts that make § 2701, not § 2511, applicable here. Moreover, a careful reading of the full text of the *Steiger* opinion's explanation of what constitutes an interception, including a critically important sentence that was deleted when quoted in the *Pharmatrak* opinion and the government's brief, undermines rather than supports the government's appeal.

Affirmance of the district court's ruling harmonizes with all ECPA provisions, and would not reduce the limited degree of privacy against law

enforcement surveillance afforded by Title II's Stored Communications Act to electronic mail while it is in "electronic storage" in the facilities of an electronic communication service. The district court correctly noted that the pre-Patriot Act version of the ECPA applies to Councilman's conduct. The effect of the Patriot Act's amendment to the ECPA's definition of "wire communication" on the privacy of increasingly-digitized voice communications while they are in "electronic storage" the facilities of an electronic communication service is not presented here. The Patriot Act amendment to the ECPA should have no effect on this Court's interpretation or application of the pre-amendment statute to Councilman's conduct.

The inter-related constitutional doctrines of lenity and vagueness also support dismissal, because the government has arbitrarily shifted its ECPA enforcement standards, depending on whether it is the accused or the prosecutor, and the record shows that Councilman's conduct is widely and reasonably understood to be lawful.

ARGUMENT

I. THE DISTRICT COURT RULED CORRECTLY THAT AN EMPLOYEE OF AN ELECTRONIC COMMUNICATION SERVICE WHO OBTAINED THE CONTENTS OF ELECTRONIC COMMUNICATIONS WHILE THE COMMUNICATIONS WERE IN ELECTRONIC STORAGE IN THE COMPUTER FACILITIES OF THAT SERVICE, ACTED LAWFULLY UNDER 18 U.S.C. § 2701(c)(1).

The central flaws in the government's appeal are its failures to address, much less confront: (A) one of the ECPA's most fundamental, structural features: its dichotomy carefully drawn between Title I (the Wiretap Act) and Title II (the Stored Communications Act), enacting different privacy protections for various categories of communications, depending on whether or not such communications are in "electronic storage," (B) the self-servingly and unconstitutionally-contradictory positions it has taken in this and previous ECPA cases concerning the particular provisions at issue, and (C) the absence of support in ECPA text or precedent for the application of the non-statutory phrase "contemporaneous with transmission," to communications while they are in electronic storage in the facilities of an electronic communication service. §§ 2701 & 2510(17).

A. The Different Privacy Protections Afforded by Titles I and II of the ECPA Mean that Electronic Communications Cannot Be Intercepted Or "Wiretapped" When They Are In An Electronic Communication Service's Computer, Rather Than Being Transmitted From Computer to Computer Through Wires.

Although the government's brief says that Title I's Wiretap Act and Title II's Stored Communications "overlap to some degree," it is simply wrong to say that the statutory dichotomy that precludes interception of electronically stored communications is "judge made." GB 27. This appeal

founders by failing to recognize why Congress chose to enact the dichotomy between stored and non-stored communications in regulating the privacy of electronic and non-electronic communications. GB 3-7. The parties agree that both titles must be understood as integrated, internally consistent parts of the ECPA as a whole. This is particularly true because the privacy of the same communication may be regulated differently during various phases or stages, depending on whether or not it is stored at any particular time. Moreover, § 2711(1) states that, when used in the Stored Communications Act, terms defined in the Wiretap Act's lexicon, § 2510, have the same meanings.

The privacy-based distinction that divides these two titles of the ECPA is the fundamental reason why an electronic communication cannot be wiretapped or "intercepted" in violation of the ECPA's Title I, when that communication is electronically stored in an electronic communication service's computer: the ECPA's two titles afford different levels of privacy protection to an electronic communication, and different measures to implement that protection, depending on whether, at any particular time, the communication is, or is not, in "electronic storage" in the computer facilities of an electronic communication service.

1. Congress' Privacy-Based Distinction Between Stored and Never-Stored Communications.

"Wire communications" are aural transfers conveyed, in whole or in part, as electrons streaming as impulses through a wire or cable. 18 U.S.C. § 2510(1) & (18). The combination of the aural and evanescent characteristics of a "wire communication" was determined by the Supreme Court in *Katz v. United States*, 389 U.S. 347 (1967) to evoke in parties to such communications a constitutionally-protected, reasonable expectation of privacy. Put simply, *Katz* held that the privacy of a non-stored, telephone conversation is constitutionally protected from interception by government agents.

In significant contrast, electronic communications, 18 U.S.C. § 2510 (12), are not deemed to entail the same degree of expectation of privacy and, for that reason, the privacy of electronic communications is not protected from government intrusion by the Fourth Amendment. The government's *amicus* brief in *Konop* itemized the various ways that Congress indicated that electronic communications are entitled to a lesser, non-constitutional degree of privacy protection than wire communications.

> A consistent theme of the Act is that wire communications and electronic communications are treated differently, with wire communications receiving greater privacy protection than electronic communications.
>
> For example, the Wiretap Act provides a statutory suppression remedy for the unauthorized interception of wire

> communications, but contains no suppression remedy for the unauthorized interception of electronic communications. See 18 U.S.C. §§ 2515 & 2518(10)(a); Slip Op. at 230. Similarly, the Act requires high-level Justice Department approval for federal wiretap orders to intercept wire communications, but contains no such approval requirement for orders to intercept electronic communications. Compare 18 U.S.C. § 2516(1) (wire communications) with § 2516(3) (electronic communications). The Act also limits the availability of wiretap orders authorizing the interception of wire communications to cases involving the felonies specified in section 2516(1); in contrast, the federal government can obtain a wiretap order to intercept electronic communications in cases involving "any Federal felony." § 2516(3). As noted in both the 1986 House and Senate committee reports, "for non-wire, non-oral electronic communications, a different and less restrictive list of crimes can be used to justify an application for interception." H. Rep. 99-647 at 51 (emphasis added); S. Rep. 99-541 at 28 (same).

Brief for the United States As *Amicus Curiae* Supporting Appellee's Petition for Rehearing *En Banc*, February 2, 2001, at 8.

The government does not appear to have considered this question: Why are wire communications entitled to more privacy protection than electronic communications? The answer might simply be that the Supreme Court has afforded constitutional protection to the former, but not to the latter. The answer might be entirely attributable to the aural nature of wire communications, but that distinction alone does not seem adequate to justify the difference. The different levels of privacy protection are attributable, at least in part, to the fact that electronic communications are far more widely

understood and expected to be stored in the possession of non-parties as an intrinsic feature of that form of communication, as distinguished from aural, wire communications. People understand and expect that electronic mail intrinsically involves storage of their communications by an electronic communication service provider; they do not have a similar understanding or expectation when participating in aural telephone calls.

The reason that the **stored v. evanescent distinction** is a key determinant of the extent of privacy protection afforded by the ECPA to both wire and electronic communications is simply that, because of their lasting nature, stored communications are inherently more vulnerable to intrusion than evanescent communications, which must be intruded upon simultaneously with the communication, or not at all.

For this privacy-based reason, the stored v. evanescent distinction determines whether the acquisition of the content of a communication occurs through a § 2511 "intercept," or by obtaining the communication's content by a § 2701 "accessing" of a stored communication. If the content of an evanescent, non-stored wire or electronic communication is to be acquired, this must occur simultaneously with the communication, or not at all, and is an interception. This form of acquisition of the content of a telecommunication is functionally indistinguishable from the interception in

the form of "bugging" an ordinary, "oral communication" [§ 2510(2)] in a room or outdoors; if the content is not acquired simultaneously with the utterance of such an evanescent communication, it cannot be acquired at all.

In Congress' view, a lesser, non-constitutional degree of expectation of privacy can or should attach to forms of communication that are not evanescent, but rather are inherently subject to being stored by non-parties to the communication. This is certainly true of electronic communications, such as electronic mail messages, that are inherently subject to being stored by non-parties to the communication, namely § 2510(15) "electronic communication service" providers. Particularly for this case involving electronic mail, it is critical to recognize that the expectation of privacy recognized and adopted by Congress is substantially lower for a communication that: (1) inherently includes electronic storage of its contents by a non-party to the communication — an electronic communication service provider such as Interloc; (2) must be stored by the service provider before its content can be received by the intended recipient; and, (3) may be stored by the service provider even after such receipt.

A passage from § 2701(c)(1)'s legislative history indicates that access to electronic communications while "subject to the control of a third party computer operator" (i.e., control and access by employees of an electronic

communication service provider such as Interloc's Councilman), is deemed by Congress to be "authorized."

> Nevertheless, because it is subject to control by a third party computer operator, the information may be subject to no constitutional privacy protection. Thus, the information may be open to possible wrongful use and disclosure by law enforcement authorities as well as unauthorized private parties. The provider of these services can do little under current law to resist unauthorized access to communications.

S.Rep. No. 99-541, 1986 U.S.C.C.A.N. 3555, 3557, 1986 WL31829 (citation omitted). Manifestly, this passage demonstrates Congress' understanding that the parties to an email message do not have a constitutionally protected privacy interest in its content while it is in electronic storage in the facilities of an electronic communication service provider, because the third-party computer operator's control of, and access to, the communication is deemed to be "authorized." The Senate Report also states that, even though the privacy interests for communications while in the custody of a such a provider are non-constitutional, citing *United States v. Miller*, 425 U.S. 435 (1976) (customer has no standing to contest disclosure of his bank records), Congress was concerned that communications under the control of a third-party provider should not be accessible to law enforcement agents or unauthorized private non-parties to the communication without legislative controls. The report goes on to

analogize the circumstances of electronic communications stored by an electronic communications service, such as Interloc, to electronic and non-electronic financial transaction records between parties to which intermediary, non-party banks or other financial institutions have lawful access. According to the report, government and other non-party access to communications electronically stored by such an intermediary provider are regulated by Title II's Stored Communications Act in a manner modeled after the Right to Financial Privacy Act, 12 U.S.C. § 3401 *et seq*. Here, the government wrongly attempts to criminalize access to electronic communications by an employee of an electronic communication service provider. Congress intended and declared in § 2701(c)(1) that such an employee's access to communications, while in electronic storage in the facilities of such a service, is both "authorized" and lawful.

2. Wiretaps or Interceptions of Evanescent Communications Distinguished From Authorized Accessing of Stored Communications.

Title I's Wiretap Act imposes stringent requirements and controls upon law enforcement authorities that wish to "intercept" communications of participants who reasonably expect that their communication is evanescent and, for that reason, vulnerable to monitoring during the communication or not at all. Law enforcement authorities may execute an

interception only under narrow circumstances and stringent controls, including minimization. Minimization during the execution of a wiretap interception or a bug of an "oral communication" is required, because all of the communications must be monitored by human beings simultaneously with the communication (to at least some "minimal" degree) in order to identify the communications that are to be seized. Without at least some "minimal" human monitoring of all of the communications in real time, some of the targeted communications would be irretrievably lost because of their evanescent, non-stored nature. The minimization requirement is attributable to the evanescent nature of the medium of communication used by the participants. See 18 U.S.C. §2516 and 2518. By contrast, Title II's Stored Communications Act allows the government to obtain access to stored communications while they are in electronic storage in the facilities of the third-party electronic communication service under significantly less stringent requirements and controls. See § 2703-2706.

There is nothing in the ECPA, nor in case law, which limits the term, "access," when used in § 2701, to what the government calls "static acquisitions" of electronically stored communications. GB 30. Councilman cannot be prosecuted by retrospectively engrafting a newly-minted limitation into § 2701 "access." Nor is there any prohibition against an

anticipatory § 2703 order (issued as a Rule 41 anticipatory search warrant) that would authorize law enforcement authorize to access and seize of communications "in real time," upon becoming stored in an electronic communication service's computer. (Under Rule 41, the government can obtain an anticipatory search warrant to seize postal mail en route in the mail stream and before it is delivered to the addressee, or upon delivery). No minimization is required for electronic communications that are in "electronic storage," because automated means, known as "string searches" or "key word scanning," can be used to cull or sort the stored communications that are to be seized from those that are outside the scope of the § 2703 search warrant. During the execution of an anticipatory search warrant issued under § 2703, unlike a § 2518 wiretap order, no human monitor need access any communication that is not subject to seizure.

In sum, the indictment's interception charge ignores the central reason why Congress did not use the word "intercept" to describe the acquisition of communications when they are in electronic storage and thus covered by Title II, but rather used the word "access." Indeed, the government's indictment ignores the reason why the ECPA is divided into Title I and Title II at all — different levels and forms of privacy protection based on different levels of reasonable expectations of privacy depending on whether, at the

time in question, the communication is: (1) evanescent or stored and (2) intrinsically required to be stored in the facilities of an electronic communication service provider, such as Interloc.

B. The District Court Ruled Correctly That the ECPA's Interception Prohibition Applies Exclusively to the Acquisition of Electronic Communications (including email) While They Are in Transmission Through Wires From Computer to Computer, And Not While They Are in "Electronic Storage" in Computers Used to Provide Electronic Communication Service.

The District Court began its reading of the ECPA by referring to its specialized definitions of key words and phrases:

> The take-off point for the court's reasoning is the statutory definition of key terms. At the time defendant was indicted, the definitions of "wire communication" and "electronic communication" contained an important distinction. (footnote omitted). *The term "wire communication" was defined to include stored communications, while the term "electronic communication" was not*. Because of this, the Court of Appeals in *Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457 (5th Cir. 1994),* held that "Congress did not intend for 'intercept' to apply to 'electronic communications' when those communications are in 'electronic storage.'" *Id., at 461-462.*

Councilman, supra, 245 F.Supp.2d. 320 (emphasis supplied). The 5th Circuit's analysis of the pre-Patriot Act text was unquestionably correct when it stated:

> Congress' use of the word "transfer" in the definition of "electronic communication," and its omission in that definition of the phrase "any electronic storage of such communication" (part of the definition of "wire communication") reflects that Congress did not intend for 'intercept' to apply to 'electronic

> communications' when those communications are in 'electronic storage.'"

Steve Jackson Games, *supra,* 36 F.3d at 462 (emphasis supplied).

Startlingly, the only mention of the ECPA's definition of "electronic communication," 18 U.S.C. § 2510(12), in the government's brief is a single sentence that contradicts both the ECPA's text and the position that the government took when it prevailed in *Steve Jackson Games*: "**'Electronic communication' does not exclude generally communications in 'electronic storage,' as defined in the Wiretap Act. 18 U.S.C. 2510(17).**" GB 6 (emphasis supplied).

The government does not provide the slightest basis to doubt that the pre-Patriot Act version of the ECPA defined "wire communication" to include stored communications, while the term "electronic communication" did not. Neither does it provide any basis to doubt the correctness of *Steve Jackson Games*' holding that "Congress did not intend for 'intercept' to apply to 'electronic communications' when those communications are in electronic storage." *Steve Jackson Games, supra,* 36 F.3d at 461-462. In the ECPA's specialized lexicon, a "transfer" of data, such as the content of an email, does not constitute an "electronic communication" [§ 2510(12)] that is amenable to interception, "while it is in electronic storage in the facilities

of an electronic communication service." §§ 2710(c)(1) & 2510(17). Nothing in the government's brief shows that *Steve Jackson Games'* long-standing and widely-accepted analysis of the ECPA's text is incorrect.

The government's claim that its interpretation of the ECPA has not been self-contradictory, GB 28 n.7, rings hollow. When it served its interest to avoid its own interception liability in *Steve Jackson Games*, the government's understanding of the ECPA was identical to that adopted by 5th and 9th Circuits and the district court here:

> The application of Title I and Title II of the ECPA to unread private e-mail messages is straightforward. If the government acquires an unread e-mail message while it is being transmitted electronically from one computer to another, the government "intercepts" the message (18 U.S.C. § 2511(1)(a)) and is subject to the procedural and substantive requirements of Title I. In contrast, if the government seeks access to the e-mail message when it is stored on a BBS computer, or prevents the message's addressee from obtaining access to the message, it is "obtain[ing] or prevent[ing] authorized access to [the] communication while it is in electronic storage in [the] system" (18 U.S.C. § 2701(a)), and the government's actions are subject to the procedural and substantive requirements of Title II.
>
> *********
>
> As the foregoing discussion shows, the seizure of unread e-mail messages stored on a computer's hard disk simply is not an "interception" under Title I, but instead is governed by the provisions of Title II.

Brief for Appelees, United States and U.S. Secret Service, *Steve Jackson Games, Inc. v. United States,* April 11, 1994, at 13 & 18.

Here, the government stipulated that, at all material times, Interloc was an "electronic communication service" [§ 2510(15)], and that Interloc's procmail script affected messages while in its hard disk or RAM or both, just as was true of the messages electronically stored in computer facilities Steve Jackson Games, Inc. used to provide such electronic mail service to its users. When it faced $10,000-per-message liability for intercepting electronic communications while unread messages were in electronic storage in the computer facilities of Steve Jackson Games, an electronic communication service, the government persuaded the courts that it was not liable for illegally intercepting electronic mail. As Councilman's prosecutor, the government takes the opposite position.

The district court noted that the government's positions adopted here and in its *amicus curiae* participation in the *Konop v. Hawaiian Airlines, Inc.,* 302 F.3d 868 (9th Cir. 2002) were self-contradictory and, moreover, that the 9th Circuit's footnote 6 had explicitly rejected its position here: "The Government, though it apparently supported the *Konop* decision when rendered, now argues that at least a portion of that position should be ignored." *Councilman, supra* at 321.

The 9th Circuit's *Konop* panel initially held "that the Wiretap Act protects electronic communications from interception when stored to the

same extent as when in transit." 236 F.3d 1035, 1044 (9th Cir. 2000) (vacated). The government understood the panel's ruling to require law enforcement authorities to obtain a warrant authorizing interception of electronic communications when the communications were in electronic storage. The Justice Department took the unusual step of providing *amicus* support for Hawaiian Airlines' petition for rehearing. The government protested, in pertinent part:

> Moreover, requiring law enforcement to obtain a wiretap order to compel stored electronic communications would occasion a seismic shift in current practice, and substantially impair the ability of federal and state investigators nationwide to investigate criminal conduct involving electronic conduct involving electronic evidence stored on networks.[2] Under the panel's rationale, any such conduct could constitute not just a misdemeanor computer trespass, but also a five-year felony wiretapping violation, because anyone who intentionally accesses a computer without authorization and obtains information is also potentially "intercepting" an "electronic communication" in violation of 18 U.S.C. § 2511.
>
> [2] The panel's decision also dramatically expands the scope and severity of federal criminal law prohibiting unauthorized access to stored electronic communications. In addition to the misdemeanor provisions of section 2701(a), Congress specifically criminalized unauthorized access to stored electronic communications in 1996 by enacting 18 U.S.C. § 1030(a)(2)(C), which makes it a misdemeanor to intentionally access[] a computer without authorization or exceed[] authorized access, and thereby obtain[] . . . information from any protected computer if the

> conduct involved an interstate or foreign communication[.]

Brief for the United States As *Amicus Curiae* Supporting Appellee's Petition for Rehearing *En Banc*, February 2, 2001, at 10-11. Because it did not suit its purposes to say otherwise in the 9th Circuit, the government took an unqualified position: acquisition of "electronic evidence stored on networks" is not an interception. It should not be heard to say otherwise here.

Due Process forbids the government from denying Councilman the same, text-based understanding of the law that allowed it to escape interception liability in *Steve Jackson Games*, and prevent potential felony liability of government agents - had the vacated panel opinion in *Konop* not been reversed. "It is no less good morals and good law that the Government should turn square corners in dealing with the people than that the people should turn square corners in dealing with their government"); *Federal Crop Insurance Corp. v. Merrill*, 332 U.S. 380, 387-388 (1947) (Jackson, J., dissenting).

> I must emphasize in concluding that this is not an occasion to modify Justice Holmes' adjuration "men must turn square corners when they deal with the Government." *Rock Island. Ark. & La. RR. v. United States, 254 U.S. 141, 143 (1920)*. Rather, it is an occasion to emphasize that the *Due Process Clause* imposes a correlative obligation on the government when it seeks by criminal process to

> take liberty or property from a defendant: the government must establish legibly orthogonal corners for men to square.

United States v. Lachman, 2003 U.S. Dist. LEXIS 14636, *26 (D.Mass.2003) (emphasis in original).

To avoid dismissal of this charge, the government must persuade this Court that, in accepting the government's plea to rehear and vacate its prior ruling, the 9th Circuit has misunderstood the ECPA by misinterpreting and misapplying the statutory meaning of "electronic storage." The government – not the 9th Circuit – is wrong.

C. Every Word Of § 2510(17)'s Text, When Applied To The Stipulated Facts, Requires Dismissal Of the Charge.

1. Subsection (A) of § 2510(17).

As the parties' stipulation reflects, electronic mail inherently includes "Any temporary, intermediate" electronic storage of the message in each of a series of computers en route from the computer on which the message was composed to the computer(s) where it can be read by the addressee(s). The message streams from computer to computer through telecommunications wires and cables that link the series of computers together in a gigantic, worldwide "Internet."

The legal premise of the count is that, even though electronic messages were stored in the hard drives and RAM of Interloc's computers,

they could be and, in fact, were intercepted while so stored because, at the pertinent time, they were "in transmission," "in transit," or "en route" between the senders and the intended addressees. This Court should reject this premise because it is inconsistent with the ECPA's structure and text, just as the district court and 9th Circuit did.

The district court properly focused on the all-inclusive breadth of the two definitions of electronic storage in 18 U.S.C. § 2510(17), emphasizing the repeated use of the word "Any" in both subsections (A) and (B) as perhaps the strongest textual obstacle to the government's premise. The word "any" has an expansive meaning, that is, 'one or some indiscriminately of whatever kind.' " *Department of Housing and Urban Development v. Rucker*, 535 U.S. 125, 131 (2002) (*quoting United States v. Gonzales*, 520 U.S. 1, 5 (1997). Subsection (A)'s text, "Any intermediate, temporary storage of a wire or electronic communication incidental to the electronic transmission thereof," clearly applies to "any" storage in the RAM or hard drives of an electronic communication service's computer as it performs its inherent function in temporarily and intermediately processing the electronic communication. In footnote 6, the *Konop* opinion correctly observes, as does the parties' stipulation (J.App.24-25 ¶3), that "storage is a necessary incident to the transmission of electronic communications" (emphasis

supplied), and correctly concludes that "Congress understood that electronic storage was an inherent part of electronic communication" to which subsection (A) applies.

There is nothing in the ECPA's text, nor in *Steve Jackson Games*, that limits the coverage of § 2510(17)(A) to "static" storage of messages in the area on Interloc's hard disk designated as an addressee's inbox. Indeed, the legislative history's categorical statement that electronic storage includes communications while in a computer's RAM "as well storage in any other form" precludes the government's reading, because the contents of an inbox exist exclusively in the electronic communication service's hard drive. The government's brief says that what occurred in *United States v. Steiger,* 318 F.3d 1039, 1046 (11th Cir. 2003), *Steve Jackson Games* and *Konop* was a "static acquisition." GB 28-30. The government appears to be suggesting that an acquisition is "static" because when acquired, the affected communication existed in stable form on the computer's hard disk. Again, an electronic communication is in "electronic storage" whether or not it is stable or static, because "any temporary, intermediate," even momentary, storage in the computer's RAM qualifies as §2510(17)(A) storage. "Any temporary" storage cannot mean "static" or of lasting any particular interval, particularly when applied to ultra-high speed computer processing of

electronic communications. The district court's recognition that "electronic storage" may be only "momentary" is correct; the government cites nothing in the statute, or in precedents, to support a legal conclusion that "any temporary, intermediate storage" excludes momentary storage.

The 9th Circuit's reading of subsection (A) is correct for another reason. The dictionary meaning of "incidental" -- when used, as it is in subsection (A), in the phrase "incidental to" -- is "likely to happen or naturally appertaining (usually fol. by *to).*" Random House Dictionary of the English Language 2d. Ed. at 966. Thus, storage "incidental to the transmission" of an electronic communication covers storage that naturally and inherently occurs in the course of its transmission. The temporary and intermediate "store" phases of the "store-and-forward" processing of electronic mail fit, and mirror exactly, the category of "electronic storage" Congress described in § 2510(17)(A). That provision applies precisely to the "temporary, intermediate" storage events that must occur within each of the chain of computers, including Interloc's computers, as the messages proceed through the Internet's store-and-forward process, described in the stipulation, to the addressees' computers where they can be read. Indeed, it is difficult to conceive of what category of storage in RAM and/or hard drives subsection (A) refers to, if it does not refer all-inclusively to messages

stored, however temporarily and briefly, within various computers as the messages are intermediately processed for transmission through wires from the sender's computer, through various Internet-linked computers, to the addressee's computer. In short, whether read as a whole or parsed one-by-one, all of the words in subsection (A) support the rulings of the district court and 9th Circuit. Nothing in the text supports the government's position.

2. Subsection (B): "Any Storage By an Electronic Communication Service for Purposes of Backup Protection of Such Communication."

Congress recognized that, in addition to the subsection (A) category of electronic storage, which is a necessary incident of the operation of common forms of electronic communications (including electronic mail), another form of electronic storage involves storage for backup protection purposes by electronic communication service providers, such as Interloc. In order to comprehensively sweep all forms of computerized storage of electronic communications within § 2510(17)'s definition of "electronic storage," Congress included subsection (B) storage "by an electronic communication service for purposes backup protection of such communication."

3. The ECPA Creates No "Contemporaneous With Transmission" Category of Electronic Communications That Are Subject to § 2511 Interception "While In

Electronic Storage in the Facilities of an Electronic Communication Service." §§ 2701 & 2510(17).

The government's brief repeatedly claims that, even though the extra copying of Amazon-sourced communications made by Interloc's procmail script occurred while the communications were in Interloc's RAM or hard disks, or both, and not while in transmission through telecommunications cable, the copying constituted a § 2511(a)(1) interception, because Interloc acquired the communications' content "contemporaneously with transmission or transfer." The government cites nothing in the statutory text that supports its contention that the district court erred in concluding Interloc lawfully obtained access to the communications under § 2701(c)(1). In reality, its position fails to get over the following three hurdles.

First, the government must demonstrate that, even though the supposedly intercepted messages were stored in the RAM or hard drives, or both, within Interloc's computers, the stored messages were neither in subsection (A) "electronic storage," nor in subsection (B) storage. The government has yet to describe a category of stored messages that would neither be covered by subsection (A), nor subsection (B). In view of the comprehensive scope of the dual definitions of "electronic storage," when applied to electronic communications in the RAM or hard drives, or both, of

computer facilities of an electronic communication service [§§ 2701; 2510(17)], the only realistic, practical conclusion is that Congress intended all computerized storage of electronic communications within such computers to be deemed in "electronic storage." In short, there is no category of electronic communications stored in the computer facilities of an electronic communication service, such as Interloc, to which § 2511(1)(a), rather than § 2701(c)(1), applies.

Second, the "contemporaneously with transmission" phrase does not appear in the statute. If that phrase refers to the electronic processing of the message while in Interloc's RAM or hard disk, or both, it is far from clear that electronic communications are in "transmission" while in "electronic storage" under the pre-Patriot Act version of the ECPA. When the phrase initially appeared in *United States v. Turk*, *526 F.2d 654* (5th Cir.), *cert. denied,* 429 U.S. 823 (1976) and *Steve Jackson Games*, it referred to acquisition of a communication while in transmission through cable, not while stored in an electronic communication service's computer. The government's attempt to apply the phrase, "contemporaneously with transmission," to communications while in electronic storage in the computers of an electronic communication service is unprecedented and conflicts with the ECPA.

The third obstacle is that, even if such a stored, but not "electronically stored" category of electronic communications existed while in Interloc's computers, the government would have to prove that Councilman willfully agreed with others to intentionally copy them while the communications they were neither in subsection (A), nor in subsection (B) storage. The government argued successfully in *Steve Jackson Games* that no interception occurred, if the government (or, in this case, Interloc) obtained electronic mail messages while they were in the addressees' mailboxes. Hence, it must agree that *Steve Jackson Games* holds that such messages would then have been in subsection (A) electronic storage. The government cannot deny that, if the messages were copied while they existed as backup copies in Interloc's computer, they could not have been intercepted, because the content of the messages would then have been acquired while the message were in subsection (B) electronic storage. There is no nano-sized storage category, to which the interception prohibition applies. But, even if such a category of storage exists, it is preposterous in view of § 2511's specific intent requirement [*see In re Pharmatrak,* 329 F.3d 9, 22-23 (1st Cir. 2003)] to suggest that Councilman willfully agreed to intentionally acquire the contents of the messages while they were in neither (A) nor (B) electronic storage. The district court highlighted this fatal flaw in the indictment, when

it referred to the "challenge" of understandable jury instructions requiring the government prove that alleged interception conspiracy specifically intended to acquire the contents of email messages while they were in Interloc's RAM or disk, or both, but yet in neither (A) nor (B) storage in Interloc's computers.

4. Neither the *Pharmatrak* Nor the *Steiger* Case Controls Here, Because Neither Case Involved Acquisition of Communications While Electronically Stored in a § 2701 Computer and, In Any Event, the Explanation of a §2510(4) "Intercept" in Those Cases Undermines, Rather Than Supports, the Government's Appeal.

The government claims that this Court's holding explaining what constitutes an interception in *In re Pharmatrak,* 329 F.3d 9, 21-22 (1st Cir. 2003) (quoting *United States v. Steiger*, 318 F.3d 1039, 1050 (11th Cir. 2003)) "largely controls this appeal." GB 23. Pharmatrak's automatic routing program effectuated a § 2511 interception precisely because, unlike Interloc's procmail script, it did not acquire any communication "while it is in electronic storage" in a "facility through which an electronic communication service is provided," nor was it authorized by an employee of such a service, such as Councilman. § 2701(c)(1).

Not only do *Pharmatrak* and *Steiger* conclusively take Interloc's procmail script out of § 2511, they firmly place it within § 2701. In both

cases, the court decided whether § 2511 or § 2701 applied by determining whether the automated acquisition of the communications occurred while their contents were in electronic storage in the computer facilities of a § 2510(15) "electronic communication service."

In *Pharmatrak*, the issue whether to apply § 2511 or § 2701 was determined by the district court by summary judgment. *In re Pharmatrak*, 220 F. Supp. 2d 4 (D.Mass. 2002), *rev'd on other grounds*, *In re Pharmatrak*, 329 F.3d 9 (1st Cir. 2003). Plaintiffs alleged in their complaint that defendants violated § 2701 by "accessing data in plaintiffs' computers, including the content of plaintiffs' emails." *Id.* at 13. Granting defendants' motion for summary judgment, the district court held that, *inter alia*, "an individual Plaintiff's personal computer is not a 'facility through which an electronic communication service is provided' for the purposes of § 2701." *Id*. Due to its obvious correctness, the plaintiffs did not appeal that ruling.

In *Steiger*, the 11th Circuit reached the same unremarkable conclusion – that § 2701 applies where the acquisition of the communications occurred while they were in electronic storage in the computer facilities of a § 2510(15) service. Appealing the denial of his motion to suppress, Steiger argued that the act of hacking into an individual's personal computer violated § 2701. The 11th Circuit disagreed: "[§ 2701] … does not appear to

apply to the source's hacking into Steiger's computer … because there is no evidence to suggest that Steiger's computer maintained any 'electronic communication service' as defined in 18 U.S.C. § 2510(15)." *Id*. at 1049. Section 2701 would have applied, according to the court, had the hacker "accessed and retrieved any information stored with Steiger's Internet Service provider." *Id*. From *Pharmatrak* and *Steiger*, it is clear that § 2701 – not § 2511 – applies here.

Even worse, the government egregiously misinterprets *Pharmatrak's* explanation of what constitutes an interception. Far from proving that Interloc's procmail script falls "squarely within the definition of 'intercept,'" GB 24, *Pharmatrak* and the case it relies on, *Steiger*, categorically demonstrate exactly the opposite.

In *Pharmatrak*, this Court adopted the definition of an "interception" formulated by the 11th Circuit in *Steiger* by quoting *verbatim* from the opinion:

> Under the narrow reading of the Wiretap Act we adopt . . ., very few seizures of electronic communications from computers will constitute 'interceptions.' **. . .** Therefore, unless some type of automatic routing software is used (for example, a duplicate of all of an employee's messages are automatically sent to the employee's boss), interception of E-mail within the prohibition of [the Wiretap Act] is virtually impossible.

Id. at 22 (emphasis supplied). The government, in turn, quoted this passage *verbatim* (including the ellipses) in its brief, GB 25, to support the proposition that the procmail script was identical to the interception device in *Pharmatrak*. In so doing, the government, like this Court in *Pharmatrak*, replaced with ellipses the very sentence that – though irrelevant (therefore properly omitted) in *Pharmatrak*[3] – completely forecloses application of the Wiretap Act here.

The omitted sentence is this: "There is only a narrow window during which an E-mail interception may occur – the seconds or mili-seconds before which a newly composed message is saved to any temporary location following a send command." *Steiger* at 1050 (emphasis supplied). As an example of a device which could accomplish an interception in this infinitesimal window, the *Steiger* court mentioned "automatic routing software" through which "a duplicate of all of an employee's messages are automatically sent to the employee's boss." *Id*. Contrary to what the government argues, GB 25, the mere fact that a device is "automatic routing software" does not determine whether the acquisition tool works an interception. Rather, the critical question is when such a tool acquires the E-

[3] The sentence was irrelevant in *Pharmatrak* because in that case, as in *Steiger's* example of a boss automatically copying each of an employee's outgoing messages, the interception device acquired the communications' contents between the time the message was sent by the user and when it was saved in temporary storage in the facilities of an electronic communication service.

mail. Unless it does so in the "narrow window" between a send command and the saving of the message in "any temporary location" thereafter – that is, unless the acquisition occurs in the wires – there is no interception.

Read in its entirety, then, the *Steiger* court's definition of "interception" adopted by *Pharmatrak* expressly demonstrates that the procmail script could not possibly have worked an interception. The government has stipulated that the procmail script did not copy any emails until they were already saved in Interloc's RAM and/or hard drive. J.App.26 (¶ 5). As discussed *supra*, data stored in either RAM or hard drive, or both, constitute "temporary" and/or "intermediate storage" under 2510(17)(A). Once an email is saved in such a "temporary location," *Steiger* at 1050, the "narrow window" during which an interception may occur is shut. Because procmail affected stored communications, it could not possibly have worked an interception. *Pharmatrak*' reasoning does, indeed, "largely control this appeal." But it supports a conclusion exactly opposite that which the government – by misleadingly omitting the dispositive sentence – urges.

II. THE DISTRICT COURT RULED CORRECTLY THAT INTERLOC LAWFULLY ACCESSED EACH COMMUNICATION "WHILE IT [WAS] IN ELECTRONIC STORAGE" IN ITS SYSTEM UNDER §2701(c)(1).

A. The Government's "Contemporaneous with Transmission" Argument Also Founders On the Key Word, "While It Is In Electronic Storage", in §2701.

The government's appeal ignores the fact that, in enacting the ECPA, Congress understood that one of the uncanny capabilities of computers is "multi-tasking" -- the simultaneous performance of multiple operations. When used in §2701, "while" carries its ordinary meaning: simultaneously, or "at the same time." Even if Interloc's procmail script were properly described as a "siphon," its operation was lawful under §2701(c)(1) so long as it acted "while" the affected messages were simultaneously in § 2510(17)(A) or (B) storage in Interloc's system. The record confirms that this is exactly what occurred, and the government's brief presents nothing to question that conclusion.

B. The District Court's Ruling That Councilman's Conduct Was Lawful Under §2701(c)(1) Neither Degrades the Privacy of Electronic Mail, Nor Permits the Government to "Intercept" "Electronic Communications" Without a §2518 Authorization.

The Government asserts that this court must adopt its interpretation of the term "electronic storage" in order to better protect Internet privacy. This argument, like the others already discussed, falls flat. After all, under the Government's distorted interpretation of "electronic storage," Interloc (or

the Government under a § 2703 warrant) could continue to legally store, access, and read the contents of all emails passing through its server computers by configuring Procmail to copy the communication immediately *after* (rather than immediately *before)* storing a copy in the recipient's mailbox. Interloc could and did construct a program to legally copy email while stored in the backup queue of a server computer, since these backup queue copies fall within the meaning of §2510(17)(B)("'electronic storage' means…any storage of such communication by an electronic communication service for purposes of backup protection…"). The Government's proposed interpretation, therefore, does nothing to enhance privacy. Instead of limiting access to the content of stored email, it would only serve to change the methods used to access it. For privacy protection purposes, it makes no sense to make felony liability turn on whether Interloc's copies of the stored, Amazon-sourced emails were made before or after they were appended to the intended recipient's inbox. Not surprisingly, such an interpretation cannot be squared with the ECPA's text or legislative history.

In subsection (c) of 18 U.S.C. § 2701, the ECPA identifies three categories of persons and entities that may lawfully "access"…"a facility through which an electronic communication service is provided," and

thereby "obtain" a wire communication "while it is in electronic storage in such system." Subsection (c) states that such conduct is not deemed unlawful if authorized:

> (1) by the person or entity providing a wire or electronic communications service;
>
> (2) by the user of that service with respect to a communication of or intended for that user; or
>
> (3) in section 2703, or 2704, or 2518 of this title.

It is stipulated that Interloc acted in this case as an "electronic communication service." Manifestly, subsection 2701(c)(2) permits the sender or recipient of email to lawfully enter the facility (the provider's computer) and obtain or alter the content of email, but only "with respect to a communication of or intended for that user." In other words, a party to an email may enter the provider's computer to send, receive or alter email to which he or she is a party. In parallel fashion, subsection 2701(c)(3) states that a government agent or agency may enter the facility and obtain the content of email "while it is in electronic storage in that system," if authorized by an judicial order, including an order permitting electronic surveillance issued pursuant to section 2518, and orders issued pursuant to sections 2703 and 2704. Subsection 2701(c)(1) authorizes the electronic

communication service provider (here, Interloc) to obtain access to electronic mail "while it is in electronic storage in that system" just as parties to email communications and government agents armed with judicial orders are.

Notably, subsection 2701(c)(3) indicates that law enforcement agents may acquire the content of communications by entering the facilities of an electronic communication service when authorized by a §2518 interception order, or through an order under §§2703 or 2704, depending on the electronic means of surveillance and acquisition to be used by the agents. Law enforcement officers who enter the facilities of an electronic communication service to execute a § 2518 judicial order to intercept electronic communications may do so by entering such facilities to install what is commonly referred to as an Ethernet filter or sniffer, which functions much as a wiretap of an earlier era did – it filters electronic communications when they are streaming through telecommunications wires or cables.[4] This is not the same as a procmail script that acquires the communications when they are in electronic storage in a computer's RAM or hard disk, or both.

[4] The government submitted an FBI official's affidavit that states that the FBI does not "usually" use an Ethernet sniffer to effectuate electronic surveillance and that internet service providers who effectuate such surveillance under court orders do not "generally" use such a sniffer. J. App.28-29. This does not exclude the use of Ethernet sniffers, nor does it address the activities of state and federal agencies other than the FBI. Law enforcement agents may choose to deploy an Ethernet sniffer, rather than a procmail script, because information concerning the characteristics of the communications to be seized are less accessible to the internet service provider. Procmail scripts are deployed in the provider's, rather than in the government's, computer.

The Ethernet sniffer device is installed by, in effect, splicing it into the telecommunication cable upstream from the computer facilities of the electronic communication service. The Ethernet sniffer recognizes the "packets" or "packet segments" as they stream through the wire or cable, which constitute all, or portions of, the electronic messages which include the characteristics specified in the interception order (such as identifiers suspected parties to the communications and their criminal content). The Ethernet sniffer causes copies of the filtered communications to be made on a computer installed by the officers for that purpose, while allowing them and all other packets passing through the cable to proceed as if unaffected by the sniffer.

The Justice Department described this Ethernet sniffer technology when it publicized what was then called the "Carnivore System" and published an "Independent Technical Review of the Carnivore System". J.App. 150-170. It may also be downloaded from the Justice Department's Website at http://www.usdoj.gov/jmd/publications/carnivore_draft_1.pdf. This document depicts the Ethernet sniffer's architecture in Figure ES-1 at J.App 161, which also states in part: "When placed at an ISP, the collection computer receives all packets on the Ethernet segment to which it is connected and records packets or packet segments that match Carnivore

settings." "The Ethernet Tap" is further described at J.App. 168. The FBI has put this technology to use, but renamed it CSS-1000. See J. App. 170. Hence, § 2701(c)(3)'s exception for conduct authorized by a § 2518 interception order clearly applies to accessing the facilities of an electronic communication service in order to the install and operate a CSS-1000 or similar Ethernet sniffer and related interception equipment and is not, for that reason, rendered ineffective or irrelevant by the *Konop* and *Councilman* rulings.

Even if (contrary to the holding in *Steve Jackson Games)* stored electronic communications can be intercepted, Count One should be dismissed. There is nothing irrational or anomalous about Congress's choice to enact § 2701(c)(1) and (3) as it did. As the legislative history indicates, Congress recognized that the content of electronic communications, including electronic mail, is not protected from being obtained by an electronic communication service in which the communication "while it is electronic storage." Such a privacy loss was deemed consistent with the inherently insecure nature of such electronic communications, primarily because they are stored in the facilities of a non-party to the communication. The Senate Report stated that the privacy of such communications is comparable to imparting the content of a financial or credit card transaction

between a buyer and seller to a bank or the other financial institution for processing. But Congress also decided that such an inherent privacy loss need and should not extend to unauthorized intrusion by law enforcement officials. Hence, Congress decided by enacting § 2701(c) that the same conduct which is lawful when performed by Mr. Councilman would be unlawful if performed by a law enforcement official, unless authorized by a judicial order.

The Government argues that giving the statutory definition of "electronic storage" its literal meaning is inconsistent with the interception-exemption provisions of the Wiretap Act, some of which exempt electronic communication service providers from interception liability. GB 33-34 (referring to § 2511(2)(a)(i), (2)(b); 2(c), 2(d), 2(e), 2(f), (2)(g), (3)(a)). This is simply not the case, because none of the provisions apply to acquisition of communications while electronically stored in the facilities of such a provider. For example, Section 2511(2)(a)(i) merely represents an acknowledgment that an electronic communication service provider that is a telephone company must occasionally monitor the flow of traffic through its communications lines and cables in order to ensure that those conduits are functioning correctly. As the Senate Judiciary Committee explained: "The provider of electronic communications services may have to monitor a

stream of transmissions in order to properly route, terminate, and otherwise manage the individual messages they contain." S. Rep. No 99-541 at 20, reprinted in 1986 U.S.C.C.A.N. 3555, 3574 (interpreting § 2511(2)(a)(i)). Likewise, § 2511(g)(i) and § 2511(h)(ii), read in context, are nothing more than clarifications intended to give guidance to electronic service providers on the use of particular technologies in common usage at the time the ECPA was passed. See S. Rep. No 99-541 at 18, reprinted in 1986 U.S.C.C.A.N. 3555, 3572-74 (stating that the § 2511(g) and § 2511(h) were intended to clarify that the listed actions were permissible under the statute). There is no need to distort the statutory definition of § 2510(17) "electronic storage" and § 2701 that exempts providers from interception liability for obtaining access to communications while they are in computer facilities used to provide electronic communication service, in order to reconcile these provisions with Title I's exceptions to interception liability which apply to non-stored communications covered by Title I.

The government argues that "voice communications" (which are in ECPA terms §2510(1) "wire communications" made up of § 2510(18) "aural transfers") are becoming increasingly digitized, and the 9th Circuit and district court rulings would render such communications subject to uncontrolled surveillance by private sector electronic communication

services and law enforcement surveillance without § 2518 authorization. GB 39-40. The spread of damage to privacy about which the Justice Department warns is entirely due to ill-considered and hastily enacted amendments to the ECPA adopted in the Patriot Act. Congress is now considering several bills that would reconsider or repeal various provisions of the Patriot Act. As noted in *Konop, supra,* 302 F.3d at 877 n.5, prior to the Patriot Act, "wire communication" included any storage of same and, accordingly, any acquisition of a stored or non-stored "wire communication" by a non-party to the communication was then an interception. The pre-Patriot Act ECPA was in force at all times material to this case and this Court's ruling will apply solely to that version of the statute. Certainly, the privacy-damaging effect of the Patriot Act provides no basis to allow prosecution of Councilman under the pre-Patriot Act ECPA.

III. DUE PROCESS PRINCIPLES OF LENITY AND VAGUENESS REQUIRE THAT THE COUNT BE DISMISSED.

Permitting Councilman's prosecution would criminalize a broad variety of conduct that is widely and reasonably understood to be lawful. For example, when discussing the applicability of the ECPA to employers who commonly are providers of electronic communication services to their employees, one authority stated: "…e-mail is generally monitored from a

server that stores copies of the outgoing messages on the hard drives of the employee's terminals. Thus, the interception provisions of ECPA would generally not apply to employee e-mail monitoring." Internet Law for the Business Law, ABA Section of Business Law (Reiter, Blumenfeld, Boulding eds.); see also Thomas R. Greenberg, E-Mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute, 44 Am. U. L. Rev. 219, 249 (1994) ("Thus, the limitations imposed on employer interceptions of wire and electronic communications vanish once the same communication is in storage. Accordingly, in order to avoid Title III liability, an employer need only access employee communications once they have been stored."); Ruel Torres Hernandez, ECPA and Online Computer Privacy, 41 Fed. Comm. L. J. 17, 39 (1988) ("In other words, there simply is no ECPA violation if 'the person or entity providing a wire or electronic communications service' intentionally examines everything on the system, whether or not it is for the purpose of a system quality control check."). Indeed, a 2001 survey conducted by the American Management Association found that over 62% of the 1,627 employers who responded to the survey monitored internet connections (this involves filtering the *from:* and *to*: lines of email messages) and over 46% monitored the content of email messages. See J.App.96-101.

Moreover, electronic communication services, such as a typical employer who provides such services, a university that provides such services to its personnel and its students, or an internet service provider that provides such services to any member of the public (§ 2510(15) applies to all three types of providers), all use Mail Transfer Agent (MTA) software that is identical, or not materially different, from the sendmail and procmail software used by Interloc in this case to scan the *from:* line of email message in order to monitor for incoming unwanted junk mail, commonly referred to as "spam." See J.App. 123 (describing the MTA software used by Interloc, Sendmail 8.8, to filter the *from:* line of incoming messages for spam characteristics).

The district court ruled correctly that the constitutional rule of lenity supports dismissal of the count. *Liparota v. United States*, 471 U.S. 419, 427 (1985). The government's application of the ECPA to Councilman's conduct also violates due process, because it is novel and unprecedented, as well as arbitrary and capricious in view of the contrary legal positions it urged in *Steve Jackson Games* and *Konop*. *Kolender v. Lawson,* 461 U.S. 352 (1983). Without fair notice to Councilman or similarly situated persons of its novel interpretation of the ECPA, this prosecution converts into

felonies a wide range of conduct commonly and reasonably understood to be lawful. *United States v. Lanier*, 520 U.S. 259, 266 (1997).

IV. CONCLUSION

For all the foregoing reasons, the district court's order dismissing the count should be affirmed.

Respectfully submitted,

Andrew Good
BBO #201240
1st Cir. #34398
Good & Cormier
83 Atlantic Avenue
Boston, MA 02110-3711
Tel: (617) 523-5933
Fax: (617) 523-7544
agood@goodcormier.com

On the brief:
Matthew Zisow
Harvard Law School
Class of 2003
Candidate for Bar Admission, 11/03

UNITED STATES COURT OF APPEALS
FOR THE FIRST CIRCUIT

CERTIFICATE OF COMPLIANCE WITH
TYPEFACE AND LENGTH LIMITATIONS

Appeals No. 03-1383

UNITED STATES OF AMERICA
Appellant

v.

BRADFORD C. COUNCILMAN
Defendant-Appellee

TO BE INCLUDED IMMEDIATELY BEFORE THE
CERTIFICATE OF SERVICE FOR ALL BRIEFS FILED IN THIS COURT

1. This brief has been prepared using (SELECT AND COMPLETE ONLY ONE):

   [**X**] 14 point proportionally spaced, serif typeface (such as CG Times or Times New Roman. Specify software name and version, typeface name, and point size below (for example, Wordperfect 8, CG Times, 14 Point):

   [ ] 10 _ characters per inch, monospaced typeface (such as Courier or Courier New). Specify software name and version, typeface name, and character per inch below (for example, Wordperfect 8, Courier 10 _ CPI):

2. EXCLUSIVE of the corporate disclosure statement; table of contents; table of citations; addendum; and the certificate of service, this brief contains:

   [ ] _____ pages (may not exceed 30 pages for opening or answering brief or 15 pages for reply brief); OR

   [**X**] 12,854 words (may not exceed 14,000 words for opening or answering brief or 7,000 for brief reply); OR

   [ ] _____ lines of monospaced type (may not exceed 1,300 lines for opening or answering brief or 650 for reply brief; may be used ONLY for briefs prepared in monospaced type such as Courier or Courier New).

I understand that a material misrepresentation can result in the Court striking the brief or imposing sanctions. If the Court so directs, I will provide a copy of the words or line print-out.

_____
Attorney Andrew Good

CERTIFICATE OF SERVICE

I, Andrew Good, certify that I caused two copies of the Defendant-Appellee's brief and supplemental appendix to be served by hand-delivery and electronic mail, on the appellant's attorney, Gary S. Katzmann, Assistant U.S. Attorney, 1 Courthouse Way, Boston, Massachusetts 02110, on October 8, 2003.

_____

Andrew Good, Esq.
Good & Cormier
83 Atlantic Avenue
Boston, MA 02110