In the

United States Court of Appeals

For the Seventh Circuit

No. 15-2076

BARRY EPSTEIN,

Plaintiff-Appellant,

v.

PAULA EPSTEIN and
JAY FRANK,

Defendants-Appellees.

Appeal from the United States District Court for the
Northern District of Illinois, Eastern Division.
No. 14 C 8431 — **Thomas M. Durkin**, *Judge.*

ARGUED DECEMBER 10, 2015 — DECIDED DECEMBER 14, 2016

Before POSNER, MANION, AND SYKES, *Circuit Judges*.

SYKES, *Circuit Judge*. Barry Epstein sued his estranged wife, Paula, alleging that she violated the federal Wiretapping and Electronic Surveillance Act by intercepting his emails. The action arises from the couple's acrimonious divorce. Paula accused Barry of serial infidelity, so in discovery Barry asked her for all documents related to that accusation. Paula complied and produced copies of incriminating

emails between Barry and several other women. Her discovery response spawned this satellite litigation (the divorce action is still pending). Barry alleges that Paula violated the Wiretap Act by surreptitiously placing an auto-forwarding "rule" on his email accounts that automatically forwarded the messages on his email client to her.[1] He also claims that Paula's divorce lawyer violated the Act by "disclosing" the intercepted emails in response to his discovery request. The district judge dismissed the suit on the pleadings.

We affirm in part and reverse in part. The complaint doesn't state a Wiretap Act claim against Paula's lawyer. The lawyer can't be liable for disclosing Barry's *own* emails *to him* in response to *his own* discovery request. The allegations against Paula, on the other hand, technically fall within the language of the Act, though Congress probably didn't anticipate its use as a tactical weapon in a divorce proceeding.

I. Background

We take the following factual account from the amended complaint, accepting it as true for present purposes. Paula and Barry Epstein married in 1970. In 2011 Paula filed for divorce in Cook County Circuit Court, accusing her husband of infidelity. The divorce case has dragged on since then and remains unresolved. During discovery Barry's lawyer sent Paula's lawyer a document request asking for production of "[*a*]*ny and all* communications, documents, e-mails, text

[1] An email client is a computer program that is used to access and manage a user's email. The program can be installed directly on the user's computer (like Microsoft Outlook) or can be a web application (like Gmail).

messages, photographs, notes, credit card slips, bank statements, or other document whatsoever, which allegedly relate[] to [Paula's allegation of] infidelity."

Jay Frank was Paula's lawyer. In response to this document request, he produced (among other things) copies of email correspondence between Barry and several women. On the face of it, the messages seem to have been forwarded from Barry's email accounts to Paula's. This came as a shock to Barry; he inferred from this discovery response that Paula must have secretly placed a "rule" on his email accounts automatically forwarding his messages to her.

With the divorce action still ongoing, Barry filed this federal suit against Paula and Frank pursuant to 18 U.S.C. § 2520, which authorizes civil actions against persons who violate the Wiretap Act. The complaint alleges that Paula unlawfully intercepted, disclosed, and used Barry's emails in violation of the Act, and that Frank violated the Act by unlawfully disclosing and using the emails in the divorce proceeding.[2] Copies of some of the intercepted emails were attached to the complaint as exhibits.

Paula and Frank separately moved to dismiss for failure to state a claim under Rule 12(b)(6) of the Federal Rules of Civil Procedure. Both argued that intercepting an email doesn't violate the Wiretap Act unless the acquisition occurs contemporaneously with the email's transmission. The emails attached to the complaint bear date and time markings showing that they may not have been intercepted contemporaneously with their transmission. The defendants

---

[2] The suit also included a state-law claim against Paula for intrusion upon seclusion, but that claim is not important here.

argued that this date and time information was enough by itself to defeat Barry's Wiretap Act claim. Frank also argued that he can't be liable under the Act for disclosing Barry's own emails to him in response to his own discovery request in the divorce proceeding. The judge agreed with these arguments and dismissed the Wiretap Act claims against both defendants.

II. Discussion

The Wiretap Act makes it unlawful to "intentionally intercept[] [or] endeavor[] to intercept … any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a). The Act also prohibits the intentional "disclos[ure]" or "use[]" of the contents of an unlawfully intercepted electronic communication. *Id*. § 2511(1)(c), (d). "[I]ntercept" is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication." *Id*. § 2510(4). "[E]lectronic communication," in turn, is "any transfer of signs … of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system." *Id.* § 2510(12).

The parties' briefs are largely devoted to a debate about whether the Wiretap Act requires a "contemporaneous" interception of an electronic communication—that is, an interception that occurs *during transmission* rather than *after* the electronic message has "come to rest on a computer system." *United States v. Szymuszkiewicz*, 622 F.3d 701, 703 (7th Cir. 2010). Several circuits have held that the Wiretap Act covers only contemporaneous interceptions—understood as the act of acquiring an electronic communication in transit—rather than the acquisition of stored electronic communications, which is addressed by the Stored Communications Act. *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d

107, 113 (3d Cir. 2003); *United States v. Steiger*, 318 F.3d 1039, 1047 (11th Cir. 2003); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002); *Steve Jackson Games, Inc. v. Secret Serv.*, 36 F.3d 457 (5th Cir. 1994). We noted this trend in *Szymuszkiewicz* but had no occasion to decide whether we agreed. 622 F.3d at 705–06. We do not need to take a position today. Even if the Wiretap Act covers only contemporaneous interceptions, Barry has stated a Wiretap Act claim against Paula, and dismissal of the claim against her was error.

The amended complaint alleges that Paula's interception of his emails "was contemporaneous with the transmission insofar as the electronic messages destined for [Barry] were forwarded to [Paula] at the same time they were received by [Barry's email] servers." The defendants insist that the emails attached to the complaint decisively show that the interception was *not* contemporaneous.

A plaintiff can "plead himself out of court by pleading facts that show that he has no legal claim." *Atkins v. City of Chicago*, 631 F.3d 823, 832 (7th Cir. 2011). This can occur when the complaint includes "facts that establish an impenetrable defense to its claims." *Hecker v. Deere & Co.*, 556 F.3d 575, 588 (7th Cir. 2009) (quoting *Tamayo v. Blagojevich*, 526 F.3d 1074, 1086 (7th Cir. 2008)). Put slightly differently, "[a] plaintiff pleads himself out of court when it would be necessary to contradict the complaint in order to prevail on the merits." *Id*. Although the defendants strenuously argue otherwise, the emails attached to the complaint do *not* conclusively defeat Barry's allegation that Paula intercepted his emails contemporaneously with their transmission.

The emails appear to come from one of Paula's email clients. Those that were *sent* from Barry's account to the other

women show the time his email client sent the message; the emails he *received* from the other women show the time his email client received the message. Each email also shows the time Paula's email client received the forwarded message from Barry's account.[3] The district judge read these "sent" and "received" markings in the defendants' favor, noting that there are gaps between the time Barry sent or received an email and the time Paula received the forwarded email. The judge observed that "[t]he shortest interval between an original email[] and the email forwarding it to Paula's account[] is approximately three hours." Although this reasoning seems sensible on its face, there are three independently sufficient reasons why the time markings on the emails do not establish an "impenetrable defense" to the Wiretap Act claims.

First, the judge misunderstood when an interception occurs. He assumed that the time Paula's email client received the forwarded emails was the moment of interception. Although this interpretation of "interception" is understandable, we explained in *Szymuszkiewicz* that the interception of an email need not occur at the time the wrongdoer *receives* the email; in *Szymuszkiewicz* "[t]he copying *at the server* was the unlawful interception." 622 F.3d at 704. Because Barry's case was dismissed on the pleadings, we do not know how Paula's auto-forwarding rule worked. For example, we cannot tell if a server immediately copied Barry's emails—at which point the interception would be complete—even though Paula's email client may not have received them until later.

---

[3] These times are displayed down to the nearest minute.

Second, the judge mistakenly conflated the emails Barry *received* and those he *sent*. If we assume that the Wiretap Act prohibits only contemporaneous interceptions, the Act would apply to the acquisition of emails before they "cross[] the finish line of transmission," which happens when their intended recipient actually receives them. *United States v. Councilman*, 418 F.3d 67, 80 (1st Cir. 2005) (en banc).

Putting aside the general problem of determining precisely when an interception occurs, for the emails Barry *received* from the other women, it seems reasonable to compare the time Barry received the message and the time the email was successfully forwarded to Paula. But that logic doesn't apply to emails Barry *sent* to the other women. The time markings on those emails tell us nothing about *when transmission of the emails was complete*. To know that we would need to know when the intended recipients—the women Barry was corresponding with—actually received the emails. The exhibit attached to the complaint includes a few email chains that do give this information, but for many of the emails Barry sent, it's impossible to know when the intended recipients received them.[4] Because these emails don't conclusively establish when the transmissions were

[4] Take, for example, one email that appears to have been forwarded by Barry from his business email account to his personal email account and also forwarded (perhaps from the Sent folder on Barry's business account) to Paula. Paula's email client appears to have received it two minutes after the message was forwarded from Barry's business email account to his personal account. Because it's impossible to know when Barry's personal account received the email, it is well within the realm of possibility that Paula received the forwarded email first. If so, Paula's acquisition of that email would be a contemporaneous interception: Paula would have received the email before its intended recipient did.

completed, it's possible that they were intercepted contemporaneously.

Finally, it's highly unlikely that the exhibit attached to the complaint contains all the emails that were forwarded to Paula's email addresses. It's difficult to imagine what filtering algorithm Paula's auto-forwarding rule could have used that would have limited the interception to the small collection of email messages that are contained in the exhibit. Barry alleges that Paula's auto-forward rule was in place for as long as five years; it's more likely that these few dozen emails are only a small fraction of a much larger volume.

Because the emails attached to the complaint do not conclusively establish that there was no contemporaneous interception, Barry did not plead himself out of court. The judge was wrong to dismiss the case against Paula on this ground.

On the other hand, the claim against Frank (Paula's lawyer) fails for an independent reason. The complaint alleges that Frank "disclosed and used" the contents of the intercepted communications in violation of § 2511(1)(c) and (d). More specifically, Barry advanced two alternative theories of liability against the lawyer: (1) Frank "disclosed" the contents of the emails when he produced them in response to the discovery request and (2) Frank "used" them in connection with the divorce litigation to embarrass Barry. The judge rejected both of these arguments and was right to do so.[5]

---

[5] For the first time on appeal Barry offers an additional theory: Frank "disclosed" the contents of the emails to other members of his firm. This new theory is unsupported by the allegations in the amended complaint.

The disclosure theory fails because Barry already knew the contents of the intercepted emails and indeed invited their disclosure by requesting them in discovery in the divorce action. The Wiretap Act doesn't prohibit the interception of electronic communications with consent. *See* § 2511. It's true that this provision does not explicitly address the effect of express or implied consent on an alleged unlawful "disclosure" or "use" (as distinct from an alleged unlawful "interception"). *See United States v. Wuliger*, 981 F.2d 1497, 1508 (6th Cir. 1992) ("The statute does not expressly provide a 'consent to use' exception to section 2511(1)(d)."). But to "disclose" something means "[t]o make (something) known or public; to show (something) after a period of inaccessibility or of being unknown; to reveal." *Disclose*, BLACK'S LAW DICTIONARY (10th ed. 2014). Frank did not publicly disclose Barry's emails, and their content was hardly unknown to Barry. Accordingly, even if the emails were unlawfully intercepted, Frank did not unlawfully disclose their content by producing them in response to Barry's discovery request. That Frank delivered the emails to Barry's attorney and not Barry himself is irrelevant. Barry's attorney *was* Barry for purposes of the response to the discovery request.

The use theory fails for a more prosaic reason: The complaint doesn't identify any use Frank actually made of the emails. Rather, it alleges that Frank *intended* to use the emails

---

We generally permit a plaintiff appealing a Rule 12(b)(6) dismissal to "elaborate on his factual allegations so long as the new elaborations are consistent with the pleadings." FED. R. CIV. P. 12(b)(6); *Geinosky v. City of Chicago*, 675 F.3d 743, 745 n.1 (7th Cir. 2012). But this latitude is not unlimited. Barry took the opportunity to amend his complaint and could have included this allegation if there was an adequate factual basis for it.

to embarrass Barry during the divorce litigation—in cahoots with Paula and with the aim of extracting a favorable financial settlement. But the Wiretap Act does not prohibit inchoate intent.

Accordingly, we AFFIRM the judgment to the extent that it dismissed the case against Frank. The amended complaint states a Wiretap Act claim against Paula; to that extent the judgment is REVERSED, and the case is REMANDED for further proceedings.

POSNER, *Circuit Judge*, concurring. I agree with Judge Sykes that under the existing understanding of the Federal Wiretap Act Paula Epstein violated it if she searched her husband's computer for evidence of adultery by him that she could use against him in divorce proceedings, without having obtained his consent to her accessing his computer. I write separately to raise a question that neither party addresses and is therefore not before us on this appeal—whether the Act *should* be thought applicable to such an invasion of privacy; for if not the husband's suit should be dismissed.

Obviously not all claims of privacy are or should be protected by law. Virtually every adult in a society such as ours values his or her privacy, but it doesn't follow that privacy is always, or even primarily, a social good, which is to say a good that promotes social welfare. "Privacy" means concealment of facts about a person. Often such concealment serves a social purpose—an example is concealing the fact that one is on the verge of inventing a new product or process that will be patentable and make the inventor wealthy; premature disclosure might enable competitors to exploit the invention to the detriment of the inventor, thus discouraging invention. But often the facts sought to be concealed in the name of privacy are facts that, being disreputable, would if disclosed publicly tarnish a person's reputation and by doing so perhaps diminish his or her social and professional welfare and opportunities. The motive of concealment in such a case is understandable, but if the concealment is of genuine misconduct, I am unclear why it should be protected by the law. I don't understand why law should promote

dishonesty and deception by protecting an undeserved, a rightly tarnished, reputation.

Among the facts routinely attempted to be concealed for disreputable reasons is of course marital infidelity. Mr. Epstein wanted to conceal his infidelity from his wife primarily it seems because the revelation of it would give her added leverage in a divorce proceeding. I don't understand why federal, or for that matter state, law should protect an interest so lacking in any social benefit, especially when one considers that adultery remains a crime in 20 of the nation's 50 states—including Illinois, see 720 ILCS 5/11-35, where the parties reside—though it is a crime that is very rarely prosecuted. We might compare Mrs. Epstein to a bounty hunter—a private person who promotes a governmental interest. She has uncovered criminal conduct hurtful to herself, and deserves compensation, such as a more generous settlement in her divorce proceeding.

Her husband's suit under the Federal Wiretap Act is more than a pure waste of judicial resources: it is a suit seeking a *reward* for concealing criminal activity. Had the issue been raised in the litigation, I would vote to interpret the Act as being inapplicable to—and therefore failing to create a remedy for—wiretaps intended, and reasonably likely, to obtain evidence of crime, as in this case, in which the plaintiff invoked the Act in an effort to hide evidence of his adultery from his wife.