

# e-commerce law reports

**FEATURED ARTICLE**  
v9 i5



cecile park publishing

Head Office UK Cecile Park Publishing Limited, 17 The Timber Yard, Drysdale Street, London N1 6ND  
tel +44 (0)20 7012 1380 fax +44 (0)20 7729 6093 info@e-comlaw.com  
[www.e-comlaw.com](http://www.e-comlaw.com)

## Murray v Financial Visions, Inc.

No. CV-07-2578-PHX-FJM, District Court Arizona, 7 November 2008 (opinion)

A US court rules that no interception of electronic communications can occur for the purposes of liability under the Wiretap Act once the communication is in electronic storage, and if in storage, interception is covered by the Stored Communications Act.

The law governing third parties' access to private internet communications has been a perennial source of confusion for service providers and lawyers. Courts have struggled to resolve whether an email acquired by a third party during the process of transmission from sender to recipient is subject to the strict rules of the Wiretap Act<sup>1</sup>, or the less stringent provisions of the Stored Communications Act (SCA)<sup>2</sup>, both of which are parts of the Electronic Communications Privacy Act. The confusion arises from the fact that every email is actually stored temporarily - usually only for milliseconds - numerous times between the time it leaves the sender and the time it arrives in the recipient's inbox. Thus, when a third party - whether a duly authorized police officer, a hacker, an employee of the service provider, or someone else - obtains that email during transmission, it is not always clear whether that acquisition was an 'intercept' governed by the Wiretap Act, an acquisition of an email 'in storage' governed by the SCA, or both.

In *Murray v Financial Visions, Inc.*<sup>3</sup>, the US District Court for the District of Arizona recently revisited this question. The court found that the acquisition of email during transmission will almost always involve access to email in temporary storage and therefore fall within the purview of the SCA and not the Wiretap Act. This is in direct conflict with a decision by the First Circuit, *United States v. Councilman*<sup>4</sup>. However, the *Murray* court also stated that 'certain email interceptions may still fall within the Wiretap Act'<sup>5</sup>, further muddying the already opaque waters. Until this issue is resolved by the Supreme Court or the statutes are amended by Congress, the confusion is likely to continue.

### Background

The Wiretap Act states that any person (other than authorized government officials, the parties to a communication, and communications service providers) who 'intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication' shall be subject to fines, imprisonment, and/or civil suits<sup>6</sup>. 'Intercept' has been interpreted by courts as applying only to the acquisition of communications during the transmission process<sup>7</sup>. The SCA creates similar penalties for intentional, unauthorized access to 'a wire or electronic communication while it is in electronic storage'<sup>8</sup>. However, the minimum civil damages available under the Wiretap Act are generally greater than those available under the SCA. The Wiretap Act's exemption for service providers is also narrower than the SCA's<sup>9</sup>.

When it comes to government investigations, the Wiretap Act sets stricter rules for intercepting email communications than the SCA does for accessing stored emails. Thus, the SCA permits the government to obtain emails stored for 180 days or less with a search warrant based on probable cause to believe a crime has been or is being committed<sup>10</sup>. Emails stored for longer can be obtained more easily, with a court order based on a showing that the emails are 'relevant and material' to an ongoing criminal investigation or with a mere subpoena (as long as notice is first given to the subscriber of the email service, absent authorization to delay notification)<sup>11</sup>. In contrast, an intercept or 'wiretap' order can be obtained only upon a showing of probable cause to believe that one of a list of enumerated serious

crimes has been or is being committed, and only if the government can state that other investigative methods have been tried and were unsuccessful or would be unlikely to succeed or would be too dangerous<sup>12</sup>. Wiretap orders also require the government to 'minimize' (i.e., not record, or delete) the interception of communications unrelated to the crime under investigation<sup>13</sup>. The difference between 'intercepting' an email in transmission and accessing it while in storage is thus a significant one for the government, as well as private actors.

The confusion about whether an email is in transmission or storage stems from a combination of the nature of electronic communications and the statutes' expansive definition of 'electronic storage'. When a person sends an email, the email is split into 'packets', which are then transmitted from computer to computer over the internet. At several points along the way, the packets are reassembled, temporarily stored, and then repackaged and sent along toward the destination. Every email thus moves temporarily in and out of storage as it moves from the sender to the recipient's inbox. Yet, this entire process normally takes only seconds, meaning that each storage point might last only milliseconds. The Wiretap Act and the SCA, however, define 'electronic storage' broadly, as including 'any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof'<sup>14</sup>. Thus, if the definition is read literally, the SCA would appear to cover not only the acquisition of emails 'stored' by the recipient in his inbox (or the sender's outbox) after the transmission, but also the interception of an email while it

was still in the process of transmission, since intercepts would normally occur at a place of temporary storage.

If such a reading is correct, then one of two odd outcomes follows, either:

- the Wiretap Act and the SCA are redundant when it comes to acquiring emails in transmission - which makes it difficult to explain why Congress provided for greater damages under the Wiretap Act than the SCA, or why Congress made it more difficult for the government to get a wiretap order than an order for stored emails in criminal investigations; or
- the Wiretap Act simply does not apply to the vast majority of emails - which does not seem at all what Congress intended when it included electronic communications within the Wiretap Act's definition of 'intercept'<sup>15</sup>.

The First Circuit has essentially taken the first approach, holding (in an *en banc* decision) that access to email messages stored temporarily as part of the transmission process is covered by the Wiretap Act as well as the SCA<sup>16</sup>. The court there found that neither the terms of the Wiretap Act nor traditional canons of statutory interpretation clearly resolved the issue. The court therefore resorted to the legislative history to divine Congress' intent. The court found 'no indication' that Congress 'meant to exclude the type of storage used during transmission' from the Wiretap Act's scope. The court concluded that the term 'electronic communication' included 'transient electronic storage that is intrinsic to the communication process for such communications'. Since the communications at issue were 'electronic communications', according to the court, they fell under the scope of the Wiretap

Act. The court also rejected the argument that because the acquisition of emails in storage is explicitly covered by the SCA, such acquisition could not simultaneously be governed by the Wiretap Act. The court concluded that both statutes could cover the same conduct, and the government could choose which one to prosecute under.

### Ruling

In *Murray v Financial Visions*, however, a district court in Arizona ruled that unauthorized access to email stored temporarily during transmission is subject only to the SCA, and not the Wiretap Act. Patricia Murray, her husband Robert Ortiz and their business, Murray Financial LLC, sued Principal Financial Group, Inc - for which Ms. Murray sold 'securities and other investment products' - and Financial Visions, Inc. - which provided the plaintiffs with website and email services and was one of Principal's approved vendors<sup>17</sup>. In an apparent effort to comply with US Securities and Exchange Commission record-keeping requirements, Principal requested that Financial Visions and other approved vendors 'intercept and automatically transmit all email sent from or received by any Principal representatives', including Ms. Murray<sup>18</sup>. After Ms. Murray learned that her emails had been intercepted, she, her husband and their company filed a putative class action for violations of the Wiretap Act against Principal, Financial Visions and the other approved vendors. However, the plaintiffs did not allege any violations of the SCA. The defendants moved for judgment on the pleadings, arguing that the plaintiffs 'failed to state a valid claim under the Wiretap Act because the intercepted email messages were in 'electronic storage'...and therefore

were not subject to the Wiretap Act'<sup>19</sup>.

Relying on the Ninth Circuit's ruling in *Konop v. Hawaiian Airlines, Inc.*<sup>20</sup>, a case involving unauthorized access to a secure website, the court in *Murray* held that an interception of electronic communications is unlawful under the Wiretap Act only if it is 'acquired during transmission, not while it is in electronic storage'<sup>21</sup>. Thus, '[n]o interception can occur, for purposes of liability under the Wiretap Act, once the communication is in 'electronic storage'<sup>22</sup>. However, the court continued, '[e]mail and other electronic communications are stored at various junctures in various computers between the time the sender types the message and the recipient reads it'<sup>23</sup>. Therefore, the court reasoned, any acquisition of an email while it is in this 'temporary, intermediate' storage 'incidental to the electronic transmission' is covered only by the SCA - and not the Wiretap Act<sup>24</sup>.

The court recognized that this meant that 'the Wiretap Act would have "virtually no effect" on email interceptions'<sup>25</sup>, since most emails would be accessed from a point of temporary storage. However, relying on a decision by the Eleventh Circuit, the court found that '[t]here [remains] a narrow window during which an E-mail interception may occur—the seconds or milli-seconds [sic] before which a newly composed message is saved to any temporary location following a send command'<sup>26</sup>. The court therefore concluded that 'even under the narrow reading adopted by the Ninth Circuit, certain email interceptions may still fall within the Wiretap Act'<sup>27</sup>. Because the plaintiffs had not alleged that any of the intercepted email 'was ever in electronic storage', the court held that it was 'not prepared at this

early stage of the proceedings to conclude as a matter of law that [the plaintiffs'] email transmissions necessarily involved 'electronic storage' so as to defeat [their] claims<sup>28</sup>. Accordingly, the court denied the defendants' motion for judgment on the pleadings.

The differences among the courts over how to reconcile the 'complex, often convoluted' intersection of the Wiretap Act and the SCA<sup>29</sup>, are likely to continue until the courts of appeals come to a consensus, the Supreme Court resolves the issue once and for all, or Congress amends the statutes. In the meantime, service providers and lawyers will need to tread carefully when confronted with the issue of whether the acquisition of email by government agent, a hacker, or some other party is covered by the Wiretap Act, the SCA, or both.

---

**Michael Vatis** Partner  
Steptoe & Johnson LLP  
mvatis@steptoe.com

---

1. 18 U.S.C. §§ 2510-2522.
2. 18 U.S.C. §§ 2701-2712.
3. No. CV-07-2578-PHX-FJM (D. Ariz. 7 November 2008) (slip op.).
4. 418 F.3d 67 (1st Cir. 2005).
5. Murray, slip op. at 9.
6. 18 U.S.C. §§ 2511 (1)(a), 2520(a).
7. The Wiretap Act's definition of 'intercept' is actually not very clear, as it defines the term simply as 'the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device', without any reference to acquisitions of communications in transmission or in storage (18 U.S.C. § 2510 (4)). Nevertheless, courts have generally held that 'intercept' applies to the acquisition of communications only during the transmission process, not while in storage. See *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002).
8. 18 U.S.C. §§ 2701 (a), 2707 (a).
9. Compare 18 U.S.C. § 2511(2)(a)(i) (exempting from the prohibition those interceptions by a communications service provider that are 'a necessary incident to the rendition of his service or to the protection of the rights or property of the provider') with id. § 2701(c) (broadly exempting from the SCA's prohibition any 'conduct authorized...by

the person or entity providing a wire or electronic communications service').

10. See 18 U.S.C. § 2703(a).
11. Id. § 2703(a), (b).
12. See 18 U.S.C. § 2516.
13. See id. § 2518.
14. 18 U.S.C. § 2510 (17)(A).
15. See 18 U.S.C. § 2510(4).
16. See *United States v. Councilman*, 418 F.3d 67 (1st Cir. 2005).
17. See Murray, slip op. at 2.
18. Id.
19. Id. at 8.
20. 302 F.3d 868, 874 (9th Cir. 2002).
21. Murray, slip op. at 9 (quoting *Konop*, 302 F.3d at 878).
22. Id. (quoting *Konop*, 302 F.3d at 878).
23. Id. (quoting *Konop*, 302 F.3d at 879 n.6).
24. Id. (quoting *Konop*, 302 F.3d at 879 n.6).
25. Id., (quoting *Konop*, 302 F.3d at 879 n.6).
26. Id. (quoting *United States v. Steiger*, 318 F.3d 1039, 1050 (11th Cir. 2003)), citation omitted.
27. Id.
28. Id. at 10.
29. *Konop*, 302 F.3d at 874.



# cecile park publishing

Head Office UK Cecile Park Publishing Limited, 17 The Timber Yard, Drysdale Street, London N1 6ND  
tel +44 (0)20 7012 1380 fax +44 (0)20 7729 6093 info@e-comlaw.com  
[www.e-comlaw.com](http://www.e-comlaw.com)

Registered number 2676976 Registered address 141 Wardour Street, London W1F 0UT VAT registration 577806103

## e-commerce law & policy

Many leading companies, including Amazon, BT, eBay, FSA, Orange, Vodafone, Standard Life, and Microsoft have subscribed to ECLP to aid them in solving the business and legal issues they face online.

ECLP, was nominated in 2000 and again in 2004 for the British & Irish Association of Law Librarian's Legal Publication of the Year.

**A twelve month subscription is £420 (overseas £440) for twelve issues and includes single user access to our online database.**

## e-commerce law reports

You can now find in one place all the key cases, with analysis and comment, that affect online, mobile and interactive business. ECLR tracks cases and regulatory adjudications from around the world.

Leading organisations, including Clifford Chance, Herbert Smith, Baker & McKenzie, Hammonds, Coudert Brothers, Orange and Royal Mail are subscribers.

**A twelve month subscription is £420 (overseas £440) for six issues and includes single user access to our online database.**

## data protection law & policy

You can now find in one place the most practical analysis, and advice, on how to address the many problems - and some opportunities - thrown up by data protection and freedom of information legislation.

DPLP's monthly reports update an online archive, which is an invaluable research tool for all those who are involved in data protection. Data acquisition, SMS marketing, subject access, Freedom of Information, data retention, use of CCTV, data sharing and data transfer abroad are all subjects that have featured recently. Leading organisations, including the Office of the Information Commissioner, Allen & Overy, Hammonds, Lovells, BT, Orange, West Berkshire Council, McCann Fitzgerald, Devon County Council and Experian are subscribers.

**A twelve month subscription is £390 (public sector £285, overseas £410) for twelve issues and includes single user access to our online database.**

## world online gambling law report

You can now find in one place analysis of the key legal, financial and regulatory issues facing all those involved in online gambling and practical advice on how to address them. The monthly reports update an online archive, which is an invaluable research tool for all those involved in online gambling.

Poker, payment systems, white labelling, jurisdiction, betting exchanges, regulation, testing, interactive TV and mobile gaming are all subjects that have featured in WOGLR recently.

Leading organisations, including Ladbrokes, William Hill, Coral, Sportingbet, BskyB, DCMS, PMU, Orange and Clifford Chance are subscribers.

**A twelve month subscription is £520 (overseas £540) for twelve issues and includes single user access to our online database.**

## world sports law report

WSLR tracks the latest developments from insolvency rules in football, to EU Competition policy on the sale of media rights, to doping and probity. The monthly reports update an online archive, which is an invaluable research tool for all involved in sport.

Database rights, sponsorship, guerilla marketing, the Court of Arbitration in Sport, sports agents, image rights, jurisdiction, domain names, ticketing and privacy are subjects that have featured in WSLR recently.

Leading organisations, including the England & Wales Cricket Board, the British Horse Board, Hammonds, Fladgate Fielder, Clarke Willmott and Skadden Arps Meagre & Flom are subscribers.

**A twelve month subscription is £520 (overseas £540) for twelve issues and includes single user access to our online database.**

- Please enrol me as a subscriber to **e-commerce law & policy** at £420 (overseas £440)
- Please enrol me as a subscriber to **e-commerce law reports** at £320 (overseas £440)
- Please enrol me as a subscriber to **data protection law & policy** at £390 (public sector £285, overseas £410)
- Please enrol me as a subscriber to **world online gambling law report** at £520 (overseas £540)
- Please enrol me as a subscriber to **world sports law report** at £520 (overseas £540)

**All subscriptions last for one year. You will be contacted at the end of that period to renew your subscription.**

Name

Job Title

Department  Company

Address

Address

City  State

Country  Postcode

Telephone  Fax

Email

**1** Please **invoice me**  Purchase order number

Signature  Date

**2** I enclose a **cheque** for the amount of

made payable to 'Cecile Park Publishing Limited'

**3** Please debit my **credit card**  VISA  MASTERCARD

Card No.  Expiry Date

Signature  Date

VAT No. (if ordering from an EC country)

Periodically we may allow companies, whose products or services might be of interest, to send you information. Please tick here if you would like to hear from other companies about products or services that may add value to your subscription.

priority order form

FAX +44 (0)20 7729 6093

CALL +44 (0)20 7012 1380

EMAIL [dan.towse@e-comlaw.com](mailto:dan.towse@e-comlaw.com)

ONLINE [www.e-comlaw.com](http://www.e-comlaw.com)

POST Cecile Park Publishing 17 The Timber Yard, Drysdale Street, London N1 6ND