

**Boston University**  
**Journal of Science & Technology Law**

**Legal Updates**

**Updates in Science & Technology Law —  
Communications and Privacy**

**Gwendylan Tregerman**



Cite to this column as: 1 B.U. J. Sci. & Tech. L. 10. Pin cite using the appropriate paragraph number. For example, the first paragraph of this column would be cited as: 1 B.U. J. Sci. & Tech. L. 10 para. 1.

Copyright © 1995 by The Trustees of Boston University. Except as otherwise provided, the individual authors have granted permission for copies of their respective works to be made for classroom use, provided that (1) the author and journal are identified, (2) proper notice of copyright is affixed to each copy, and (3) the *Boston University Journal of Science & Technology Law* is notified prior to its use.

1. The Eighth Circuit recently held that interactive electronic communication between school districts will not satisfy desegregation requirements. *Jenkins v. Missouri*, 36 F.3d 457 (8th Cir. 1994). African-American students brought a class action suit alleging that the school district had denied them admission based on their race. The court found inadequate as a remedy to segregation a plan utilizing SHARE NET and computer faxes to link schools in different school districts. For the Eighth Circuit, the "classroom of the future" was not an adequate remedy for physical segregation.

\*\*\*\*

2. The Ninth Circuit ruled that e-mail does not qualify as a business record to overcome hearsay objections to admissibility under Federal Rule of Evidence ("FRE") 803(6). *The Monotype Corp., PLC v. International Typeface Corp.*, 1994 WL 707044 to be reported at 43 F.3d 443 (9th Cir. 1994). The court reasoned that "e-mail is far less of a systematic business activity than a monthly inventory printout." 1994 WL 707044, at \*5. The court did not preclude the possibility of admissibility for email under other exceptions to the hearsay rule, but decided that the communication in question was too prejudicial under FRE 403 to be admitted into evidence.

\*\*\*\*

3. Fraudulent access to the benefits of cellular telephone accounts between local and distant carriers by means of falsified electronic serial numbers ("ESNs") violates a statutory prohibition against trafficking in counterfeited access devices. *U.S. v. Bailey*, 41 F.3d 413 (9th Cir. 1994); 18 U.S.C. § 1029 (1988). A cellular telephone places a call by transmitting its permanently assigned ESN, its assigned telephone number (Mobile Identification Number or "MIN"), and the number being called to a nearby antenna or "cell." For a local customer, the local carrier confirms that the ESN and MIN match before completing the call. To accommodate customers out of their service areas, local carriers permit telephones other than those subscribing to the local service to complete calls in "roaming" mode. At the time of defendant's activities in *Bailey*, roaming mode was more vulnerable to fraud than was the service to local subscribers. When a telephone with an out-of-area MIN placed a call, the local carrier would first determine whether there was a roaming agreement between the local carrier and the carrier responsible for the MIN (the "distant carrier"). If such a roaming agreement existed, the local

carrier would connect the call unless the ESN was found in a list of invalid ESNs known as the "negative file." In roaming mode, the local carrier could not confirm that the ESN and the MIN matched.

4. In *Bailey*, defendant modified cellular telephones to fool the local carrier into permitting calls placed by those telephones to be completed in roaming mode, even though the calls could never be billed. This scheme is known in the industry as "tumbling the ESN." The process involves altering the programming embedded in the hardware of the telephone to cause the telephone to send out random ESNs. By changing the MIN in the telephone to an out-of-area MIN, the user could force the telephone to place calls in roaming mode. Then, by transmitting any ESN not listed in the negative file, the user could trick the local carrier into connecting the call.
5. The district court granted Defendant's motion to acquit, analogizing this case to ones in which defendants had used cloning devices to receive scrambled cable channels. *U.S. v. McNutt*, 908 F.2d 561 (10th Cir. 1990). Because no one received a bill, the district court determined that the defendant had not accessed any accounts and therefore the activities of the defendant did not constitute "producing counterfeit access devices." 18 U.S.C. § 1029 (a)(1) (1988) (emphasis added).
6. An "access device" comprises "any card plate, code, account number or other means of account access that can be used ... to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument)." 18 U.S.C. § 1029(e)(1). "'Counterfeit access device' means any access device that is counterfeit, fictitious, altered, or forged, or an identifiable component of an access device or a counterfeit device." 18 U.S.C. § 1029(e)(2). Granting Defendant's motion to acquit, the district court determined that the defendant's use of falsified ESNs did not constitute "producing counterfeit access devices" within the meaning of the statute because there was no evidence that the distant carrier ever suffered a direct accounting loss. 18 U.S.C. § 1029(a)(1). The district court analogized the facts of the case to the facts of *United States v. McNutt*, 908 F.2d 561 (10th Cir. 1990), *cert. denied*, 498 U.S. 1084 (1991). *McNutt* held that the sale of satellite television descramblers that used electronic addresses "cloned" from a legitimate unit to allow decryption of pay television services did not violate section 1029

because the cloned descramblers did not debit the accounts of legitimate subscribers and that the statute did not protect against indirect economic harms caused by "free riding." *United States v. McNutt*, 908 F.2d at 564.

7. The Ninth Circuit reversed, rejecting the *McNutt* interpretation of "account access." The Court of Appeals understood "account access" to include the privileges received from a carrier by virtue of the carrier's maintenance of an account. Thus, a defendant's activities need not harm a specific subscriber to constitute a harm because either the home or the distant carrier would have to assume the cost of the call.
8. Both the Fifth and the Eighth Circuits have taken the same approach, interpreting "account access" to include an account's privileges. *United States v. Brewer*, 835 F.2d 550 (5th Cir. 1987); *United States v. Taylor*, 945 F.2d 1050 (8th Cir. 1991). In contrast, in *United States v. Brady*, 13 F.3d 334 (10th Cir. 1993), the Tenth Circuit remained committed to the *McNutt* interpretation of "account access" in the context of cellular phones modified to permit tumbling of ESNs.

\*\*\*\*

9. In *Steve Jackson Games v. U.S. Secret Service*, 36 F.3d 457 (5th Cir. 1994), the Fifth Circuit held that seizure of a computer, used to operate a bulletin board service ("BBS") and containing private e-mail that had been sent to the BBS but had not been read by the intended recipients, was not unlawfully intercepted under the Federal Wiretap Act ("FWA"), 18 U.S.C. §2510 *et seq.* (Supp. 1994). The court found that Congress did not intend the word "intercept" in the FWA to apply to electronic communications held in storage. 36 F.3d at 458.

\*\*\*\*

10. In *United States v. LaMacchia*, 871 F. Supp. 525, the defendant, David LaMacchia, established an electronic bulletin board on the Internet that allowed distant users to download popular software applications and games using the anonymous ftp file transfer protocol. A federal grand jury returned a one count indictment charging LaMacchia with conspiring with "persons unknown" to violate 18 U.S.C. § 1343, the wire fraud statute. Unlike the copyright statute, 17 U.S.C. § 506(a), the mail and wire fraud statutes do not require that a defendant be shown to have sought to personally profit from the scheme to defraud. 871 F. Supp. at 541-42. LaMacchia countered with a motion to dismiss, arguing that the

government defied the Supreme Court decision in *Dowling v. United States*, 473 U.S. 207 (1985), by resorting to the wire fraud statute to enforce the Copyright Act, 17 U.S.C. §101, *et seq.* The *Dowling* Court held that copyrighted musical compositions impressed on a bootleg phonograph are not property that is “stolen, converted, or taken by fraud” within the meaning of 18 U.S.C. § 2314, the Stolen Property Act. 473 U.S. at 214. In dismissing the indictment, the court found no conduct satisfying the fraud element of the wire fraud statute. 871 F. Supp. at 542. More importantly, the court broadly interpreted *Dowling* as distinguishing the rights conferred by copyright from the broad property interests protected by the Stolen Property Act and the mail and wire statutes. *Id.* at 543. Furthermore, in light of Congress’ fine calibration of criminal liability in the Copyright Act, copyright prosecutions should be limited to section 506 of that act. *Id.* at 545 (citing 3 *Nimmer on Copyright*, § 15.05 at 1520 (1993)). On this basis, the court held that *Dowling* precluded LaMacchia’s prosecution for copyright infringement under the wire fraud statute. 871 F. Supp. at 545.