EX PARTE OR LATE FILED

DOCKET FILE COPY ORIGINAL

May 23, 1996

Building The Wireless Future™

CTIA

Cellular Telecommunications Industry Association
1250 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20036
202-785-0081 Telephone
202-785-0721 Fax

RECEIVED

MAY 23 1996

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF SECRETARY

Mr. William F. Caton
Secretary
Federal Communications Commission
1919 M Street, NW, Room 222
Washington, DC 20554

Re: *Ex Parte* Presentation
Revision of Part 22 of the Commission's Rules Governing the Public Mobile Services
CC Docket 92-115

Dear Mr. Caton:

On Thursday, May 23, 1996, the Cellular Telecommunications Industry Association ("CTIA") represented by Mr. Randall Coleman, Vice President of Regulatory Policy and Law, Ms. Andrea D. Williams, Assistant General Counsel, and AT& T Wireless Services represented by Mr. Doug Brandon, Vice President of External Affairs and Law met with Ms. Suzanne Toller, Legal Advisor to Commissioner Rachelle Chong, to discuss cellular fraud, particularly ESN security and authentication. CTIA and AT&T Wireless also discussed issues raised in C2+ Petition for Reconsideration of Section 22.919 of the Commission's rules.

At the meetings, CTIA and AT& T Wireless Services presented the attached documents. Pursuant to Section 1.1206 of the Commission's Rules, an original and one copy of this letter along with the attachments are being filed with your office. If you have any questions concerning this submission, please contact the undersigned.

Sincerely,

Andrea D. Williams

Andrea D. Williams
Assistant General Counsel

Attachments (3)

No. of Copies rec'd 0+1
List ABCDE

Building The Wireless Future.

CTIA

Cellular Telecommunications Industry Association
1250 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20036
202-785-0081 Telephone
202-785-0721 Fax
202-736-3248 Direct Dial

Michael F. Altschul
Vice President,
General Counsel

May 16, 1996

Ms. Michele Farquhar
Chief
Wireless Telecommunications Bureau
Federal Communications Commission
2025 M Street, NW, Room 5002
Washington, DC 20554

Re: Revision of Part 22 of the Commission's Rules Governing the Public Mobile Services
CC Docket No. 92-115

Dear Ms. Farquhar:

On August 2, 1994, the Commission adopted a *Report and Order* in this proceeding implementing new Section 22.919 of the Commission's Rules to address the problem of cellular fraud. *In the Matter of Revision of Part 22 of the Commission's Rules Governing the Public Mobile Services, Report and Order,* CC Docket No. 92-115, 9 FCC Rcd. 6513 (1994).

Section 22.919 of the Rules establishes cellular equipment design specifications which require, *inter alia,* that cellular equipment's Electronic Serial Numbers ("ESNs") must be set at the equipment's manufacturing site, and must not be alterable, transferable, removable, or otherwise able to be manipulated by any party in the field. *Report and Order,* 9 FCC Rcd at 6525, ¶¶54-63. The Commission declined to make an exception to Rule 22.919 requested by some Telecommunications Industry Association ("TIA") members which would have allowed manufacturers' authorized agents to transfer ESNs in normal repair activities, and also declined CTIA's request to require that new cellular equipment comply with industry authentication standards. In addition, the Commission rejected C-Two-Plus Technologies' request for allowing the "emulation" of ESNs for "extension" phones.

After denying TIA's request for a stay of Rule 22.919 until resolution of its Petition for Reconsideration, the Commission permitted the new rule to go into effect on January 1, 1995. *See Order,* FCC 94-357, CC Docket No. 92-115, released January 10, 1995. Accordingly, both the Commission and the industry have had more than sixteen months of experience by which to measure the effectiveness of Rule 22.919. Based on that experience, CTIA urges the Commission to deny all of the pending petitions for reconsideration of this rule, including CTIA's request submitted February 2, 1995, in its *Joint Reply and Comment* filed with TIA. Simply put, the industry's experience since comments and reply comments were filed in January and February of 1995 demonstrates that there is no need to modify Rule 22.919, and therefore the Commission should reject the pending petitions for reconsideration.

It is often said that the vision of hindsight is 20-20. This proceeding affords a rare opportunity to take advantage of the clarity of this vision. With respect to the request for mandatory authentication set forth in TIA's Petition, and supported by CTIA and others on the basis that the Commission's failure to mandate authentication would delay implementation of a proven method of attacking cellular fraud, during the past sixteen months carriers and their vendors have moved aggressively to deploy authentication so that today authentication is a reality. The industry's need for authentication to combat cloning was so great that no government mandate was needed to make authentication happen. Authentication exists today in New York City, and it will be deployed in major markets throughout the United States by the end of this year. Based on the cellular industry's efforts and experience since comments were last filed in this proceeding, CTIA is confident that no rule is needed to make authentication available in all (or nearly all) cellular markets.

Similarly, TIA anticipated that modifications to Rule 22.919 would be required to avoid an adverse affect on manufacturers' repair and upgrade of cellular telephones in the field. TIA also expressed concern that adoption of the new rule would delay the introduction of new and improved cellular phones. In its February 2, 1995, *Joint Reply and Comment,* CTIA joined TIA in recommending a revision to Rule 22.919 to accommodate the manufacturers' concerns. However, the industry has been complying with the new rule for almost a year and a half, and none of these concerns have materialized. With the benefit of hindsight, CTIA now believes that no change to Rule 22.919 is required.

Finally, CTIA continues to believe that the Commission should flatly deny C-Two-Plus Technologies' request for allowing the "emulation" of ESNs for "extension" phones. Maintaining the integrity of the ESN is the cornerstone of the industry's technical efforts to preventing cellular fraud on today's analog cellular systems. The cellular industry has invested years of effort (not to mention millions of dollars) to develop and deploy three different technologies to combat cloning fraud: RF fingerprinting, velocity checking, and authentication. As AT&T Wireless Services sets forth in its May 3, 1996, *ex parte* submission in this docket, adoption of C-Two-Plus Technologies' proposed revisions to the Part 22 rules would eliminate all three of the industry's anti-fraud technologies, leaving the cellular industry with no technical weapons against cloning. This should be no surprise, since "emulation" is nothing more than a semantic ploy to avoid the word "cloning", which is the proper term to describe the conduct of duplicating a cellular phone's MIN and ESN combination.

Since "emulation" is indistinguishable on a technical basis from cloning, cellular carriers' ability to detect "emulation" is identical to their ability to detect cloning. Similarly, if the Commission were to adopt the C-Two-Plus Technologies' proposal to authorize the use of "emulated" cloned phones, carriers could not distinguish an "emulated" cloned phone from any other type of cloned phone.

Moreover, the Commission also has the benefit of hindsight with respect to this proposal. Since C-Two-Plus asked the Commission to modify its rules to permit the use of "emulated" cloned phones, a Federal District Court has clarified that what C-Two-Plus refers to as "emulation" falls squarely within the conduct prohibited by 18 U.S.C. §1029 of the U.S. Criminal Code. *See United States of America vs. Don Billy Yates, Jr., Opinion and Order,* Criminal Action 95-72 (ED Ky, Dec. 13, 1995). CTIA is not aware of any instance where the FCC rules authorize conduct that is criminalized under Title 18 of the U.S. Code.

Ultimately, the Commission must confront the reality that underlies both the technical and legal bases for denying the C-Two-Plus proposal: first, the analogy to landline telephone "extension" phones proffered by C-Two-Plus is bogus, and second, as described above, neither technology nor law enforcement can distinguish an "emulated" cloned phone from any other cloned cellular telephone.

The analogy to landline "extension" phones is flawed in numerous ways, but none so basic as the obvious fact that no matter how many terminal devices a landline customer installs on his premises to originate and terminate wired telephone service, there will be one and only one transmission path linking those devices to the telephone company's end office. In other words, landline extension phones do not afford telephone subscribers with multiple network connections and access. In contrast, cellular telephones are radios, and each cellular telephone can independently and simultaneously access a cellular system using different channels. In fact, unlike landline extension phones, there is no way multiple cellular phones simultaneously can access a single transmission path to the switch. While C-Two-Plus proposes to restrict the use of cellular "extension" phones to only one at a time, such a restriction is meaningless and unenforceable since the multiple phones (and their users) sharing the same ESN/MIN will be unable to detect if a clone is in use at the same time. This example offers yet another illustration of why the analogy to landline extension phones must fail.

For all of these reasons, CTIA does not support any change in Section 22.919, and urges the Commission to deny each of the pending petitions for reconsideration of this crucial provision of the Commission's cellular rules.

Sincerely,

Michael Altschul

Attachment

Eastern District of Kentucky
FILED
DEC 13 1995
AT LEXINGTON
LESLIE G. WHITMER
CLERK, U. S. DISTRICT COURT

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF KENTUCKY
LEXINGTON

CRIMINAL ACTION NO. 95-72

UNITED STATES OF AMERICA, PLAINTIFF,

V. OPINION AND ORDER

DON BILLY YATES, JR., DEFENDANT.

* * * * * * * * * * * * * * * *

This matter is before the Court upon the motion of the defendant, Don Billy Yates, to dismiss. This matter has been fully briefed and is ripe for review.

I. FACTS

Yates was indicted by a federal grand jury on November 2, 1995 on four counts of criminal fraud in violation of various provisions of 18 U.S.C. § 1029. Specifically, count one of the indictment charges that Yates, "knowingly and with intent to defraud, did produce, use and traffic in a counterfeit access device, which conduct affected interstate commerce," in violation of § 1029(a)(1) and (c)(1). Count two of the indictment charges that Yates "knowingly and with intent to defraud, did have control, custody, and possession of device-making equipment, which conduct affected interstate commerce," in violation of § 1029(a)(4) and (c)(1). Count three of the indictment charges that Yates "knowingly and with intent to defraud, did produce, traffic in, have control, custody and possession of a telecommunications instrument that had been modified and altered to obtain unauthorized use of telecommunications services, which conduct affected interstate commerce," in violation of § 1029(a)(5) and (c)(1). Finally, count

four of the indictment charges that Yates "knowingly and with intent to defraud, did use, have control, custody and possession of hardware and software used for altering and modifying telecommunications instruments to obtain unauthorized access to telecommunications services, which conduct affected interstate commerce," in violation of § 1029(a)(6)(B) and (c)(1). Each count alleges that the offense occurred on or about September 18, 1995. At the arraignment on November 9, 1995, Yates plead not guilty to each count.

On November 20, 1995, Yates filed two motions to dismiss the indictment. In his first motion to dismiss, Yates argues that the indictment should be dismissed as multiplicitous, or alternatively, that the United States should elect under which count of the indictment it will proceed at trial. In his second motion to dismiss, Yates argues that the indictment fails to charge him with engaging in an illegal activity. A hearing on the motions was held on December 1, 1995. The Court denied Yates' motion to dismiss the indictment as multiplicitous. However, the Court held that counts 2 and 4 of the indictment are duplicitous and ordered the United States to elect between counts 2 and 4 of the indictment. Yates' motion to dismiss on the grounds that the indictment fails to charge an illegal activity was taken under advisement by the Court.

II. YATES' MOTION TO DISMISS FOR FAILURE TO CHARGE AN ILLEGAL ACTIVITY

The issue in Yates' motion to dismiss is whether a "cloned" cellular telephone -- i.e., one with identification numbers identical to another existing legitimate unit -- falls within the ambit of § 1029. Based on representation from counsel and independent research, this appears to be an issue of first impression.

[redacted] order to determine whether the indictment charges Yates with an illegal activity, an understanding of the cellular telephone industry is imperative. Cellular telephone service is available from commercially owned and operated communications networks and is based upon a system of individual cellular telephone units having wireless radio transmission capabilities and which operate within a series of geographic "cells" served by a radio transmitter. Cellular telephones are typically programmed with two identifying code numbers, commonly referred to as the electronic serial number, "ESN," and the mobile identification number, "MIN." The ESN is a unique numerical code embedded in each cellular telephone by the manufacturer identifying that particular instrument. The MIN is a ten-digit numerical telephone number (area code + seven-digit telephone number) assigned to each cellular telephone customer. For identification purposes, both numbers are transmitted to the cellular system by the cellular telephone unit at the time a call is initiated. As the user moves from one cell to another, transmission of telephone calls is automatically shifted from one transmitter to the other, thus maintaining a consistent signal quality.

Cases construing § 1029 as it applies to the cellular telephone industry have involved "tumbling" cellular telephones. *See United States v. Brady*, 13 F.3d 334 (10th Cir. 1993); *United States v. Bailey*, 41 F.3d 413 (9th Cir.), *cert. denied*, 115 S.Ct. 2563 (1994); *United States v. Ashe*, 47 F.3d 770 (6th Cir. 1995). A "tumbling" cellular telephone is one which is capable of randomly changing either the ESN or MIN to enable the user to obtain a "free ride" through the cellular telephone system by avoiding or defeating access or billing to an individual customer account. Tumbling cellular telephones take advantage of the "roam" feature provided by cellular carriers. Cellular telephone customers may "roam," that is, place calls from a

foreign geographic cell other than the geographic cell owned and operated by the carrier with whom the customer has an account. This allows customers to place a local or long distance call from anywhere in the United States while outside the geographic area serviced by his or her home carrier. When a roamer places a call from a foreign geographical service area, the cellular telephone automatically transmits the caller's assigned ESN and MIN. In processing a roamer call, a foreign carrier immediately recognizes the MIN as belonging to another existing carrier. To provide effective customer service, roamer calls are, by internetwork agreement, practice and procedure, immediately transmitted by a foreign carrier before validation of the identifying ESN and MIN combination has been completed by a central data bank clearing house located in San Angelo, Texas. A time lag occurs while its computers seek to match the automatically transmitted identifying ESN and MIN with an existing home carrier-subscriber combination recorded in its data bank of national internetwork listings. In the absence of a valid match, all subsequent calls using the same ESN and MIN will be rejected. Although service charges resulting from unmatched ESN and MIN combinations are listed together with all pertinent information related to the call in the foreign carrier's billing computer, the illicit roaming customer cannot be identified. As a result, the charges cannot be collected from the user of a tumbling cellular telephone and the cellular carrier absorbs the cost of the call.

In *Brady*, the Tenth Circuit Court of Appeals considered whether tumbling cellular telephones are violative of § 1029. *Brady*, 13 F.3d at 338. The Tenth Circuit relied on *United States v. McNutt*, 908 F.2d 561 (10th Cir. 1990), in which the court held that cloned electronic addresses on satellite television descrambler modules were not "access devices" within the meaning of § 1029. *Id.* at 338-39. Even though the operators of satellite television services

suffered economic losses from the revenue forgone due to the use of cloned descrambler modules, the court determined that there was no violation of § 1029 because use of such modules did not "debit legitimate subscriber's accounts[, and] no additional charges accrued as a result of the unauthorized use." *McNutt*, 908 F.2d at 563-64. In other words, the court in *McNutt* held that "economic losses were not enough under § 1029; instead, the government must be able to connect actual losses to distinct transactions reflected in the company's accounting records." *Brady*, 13 F.3d at 338. Because calls made from a tumbling cellular telephone do not "debit legitimate subscriber's accounts" or "trigger the creation and maintenance of a formal record of credits and debits," the court in *Brady* held that a tumbling cellular telephone is not an access device within the meaning of § 1029. *Id.* at 339.

In addressing the identical issue in *United States v. Ashe*, 47 F.3d 770 (6th Cir. 1995), the Sixth Circuit Court of Appeals rejected the Tenth Circuit's interpretation of § 1029. In *Ashe*, the defendant challenged his conviction under § 1029 for producing and possessing a tumbling cellular telephone. In rejecting *Brady*, the court noted that "[I]n 1992, the losses charged to cellular telephone carriers resulting from 'free riding' amounted to over $100 million." *Id.* at 774. As a result, the court held that "invasion of an identifiable customer's account is not a necessary element of proof to support a conviction under [§ 1029]." *Id.* at 774. Similarly, in *United States v. Bailey*, 41 F.3d 413 (9th Cir. 1994), the Ninth Circuit Court of Appeals held that tumbling cellular telephones are access devices within the ambit of § 1029.

Unlike *Brady*, *Ashe*, and *Bailey*, Yates is charged with use, possession and trafficking of a cloned cellular telephone and cloning equipment. Cloning involves the programming of a cellular telephone so that the ESN and MIN combination is identical to a legitimate customer's

account in order to obtain free telephone service. By obtaining a cloned telephone, a cellular customer avoids an activation fee and a monthly maintenance fee charged by the cellular carrier.

The facts in this case are undisputed. In April 1995, the Secret Service executed a search warrant at a company that was selling or distributing "black boxes" that are used to clone MINs and ESNs. The search yielded a list of customers, including Yates, who had purchased at least one black box. During the same time, the Secret Service also received information from a local cellular telephone company that Yates was using a black box to clone cellular telephones. Basically, Yates' service involved providing customers with an "extension phone" so that they could have two cellular telephones with the same number, while paying the activation charge and maintenance fee for only one cellular telephone. Calls made from either cellular telephone, however, appear on the customer's bill. Yates charged $150 for his cloning service.

On September 18, 1995, Special Agent James Burch of the United States Secret Service obtained two cellular telephones, one of which was programmed with an authorized ESN and MIN, and one which was blank. Burch then contacted and arranged to meet with Yates to obtain a cloned cellular telephone. At their meeting, Yates programmed the ESN and MIN of the legitimate cellular telephone into the blank cellular telephone. Both Yates and Burch made test calls from the cloned cellular telephone. Yates was subsequently arrested and indicted for violating § 1029.

In support of his motion to dismiss, Yates argues that the Federal Communications Commission, the federal agency charged with regulating the telecommunications industry, has consistently held that telephone numbers are not the property of the carrier but are instead a public resource. *See In Re The Matter Of Administration Of North American Numbering Plan*,

[redacted] *Of The Need To Promote Competition And Efficient Use Of [redacted]trum For [redacted] Service*, FCC 86-85 (1986). As a result, Yates contends that the FCC's ruling caused ch[redacted] such as himself, to believe that the activity charged in the indictment is not illegal. Yates contends that *United States v. Levin*, 973 F.2d 463 (6th Cir. 1992), is analogous to the present case. In *Levin*, the Sixth Circuit Court of Appeals affirmed the dismissal of an indictment charging an opthamologist with Medicaid fraud for billing practices which the Healthcare Finance Administration had implied were legal. Based on *Levin* and the ruling by the FCC, Yates contends that he cannot be charged with engaging in a fraudulent activity where that fraudulent activity is wholly dependent upon ownership of a cellular telephone number by a telephone carrier.

In further support of his motion to dismiss, Yates argues that because the telephone carrier will continue to be able to bill its customers for all calls made on the extension telephone, they are not damaged by the use of the extension telephone. Moreover, Yates contends that the telephone companies have no right to profit based on the customer's use of a particular telephone number since these numbers are public resources. As a result, Yates contends that the indictment does not charge illegal activity and must be dismissed.

Yates' argument directly contradicts the legislative history of § 1029(a). In 1994, conceivably in response to the Tenth Circuit Court of Appeals' ruling in *Brady*, Congress amended § 1029(a) to specifically criminalize Yates' conduct. In passing the amendment, Congress stated:

> This section amends the counterfeit access device law to criminalize the use of cellular phones that are altered, or "cloned," to allow free riding on the cellular phone system. Specifically, this section prohibits the use of an altered telecommunications instrument, or a scanning receiver, hardware or software, to

> obtain [redacted] access to telecommunications services for the purpose of defrauding the carrier. A scanning receiver is defined as a device used to intercept illegally wire, oral or electronic communications. The penalty for violating this new section is imprisonment for up to fifteen years and a fine of the greater of the $50,000 or twice the value obtained by the offense. House Report H.R. No. 103-5271.

Clearly, Yates' conduct involved the "use of an altered telecommunications instrument . . . to obtain access to telecommunications services for the purpose of defrauding the carrier." Moreover, Yates' argument that the cellular carriers are not damaged by use of the extension telephone is erroneous. By cloning cellular telephones to enable users to have an extension phone, the cellular carriers are defrauded of the activation fee and the monthly service fee they charge for each cellular phone. Therefore, Yates' motion to dismiss will be denied.

III. CONCLUSION

Accordingly, the Court, being sufficiently advised, hereby ORDERS that Yates' motion to dismiss [docket entry 19] is DENIED.

On this 12th day of December, 1995.

KARL S. FORESTER, JUDGE

Cellular Fraud: History, Status, Technology, and Prevention

Prepared for

ederal Communications Commission

– 20 May 1996 –

Leslie D. Owens
AT&T Wireless Services

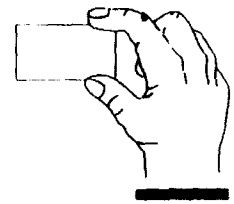
"Once you squeeze the tube, the toothpaste is out forever."

– J. Ehrlichman

"For also knowledge itself is power."

– F. Bacon

Speaker Information

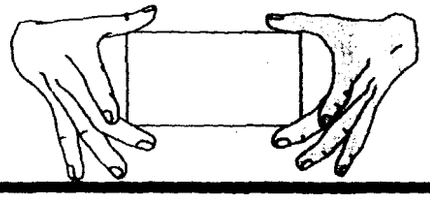


Leslie D. Owens
Director, Logical & Cross-Technology Security

AT&T Wireless Services HQ
5000 Carillon Point
Kirkland, WA 98033

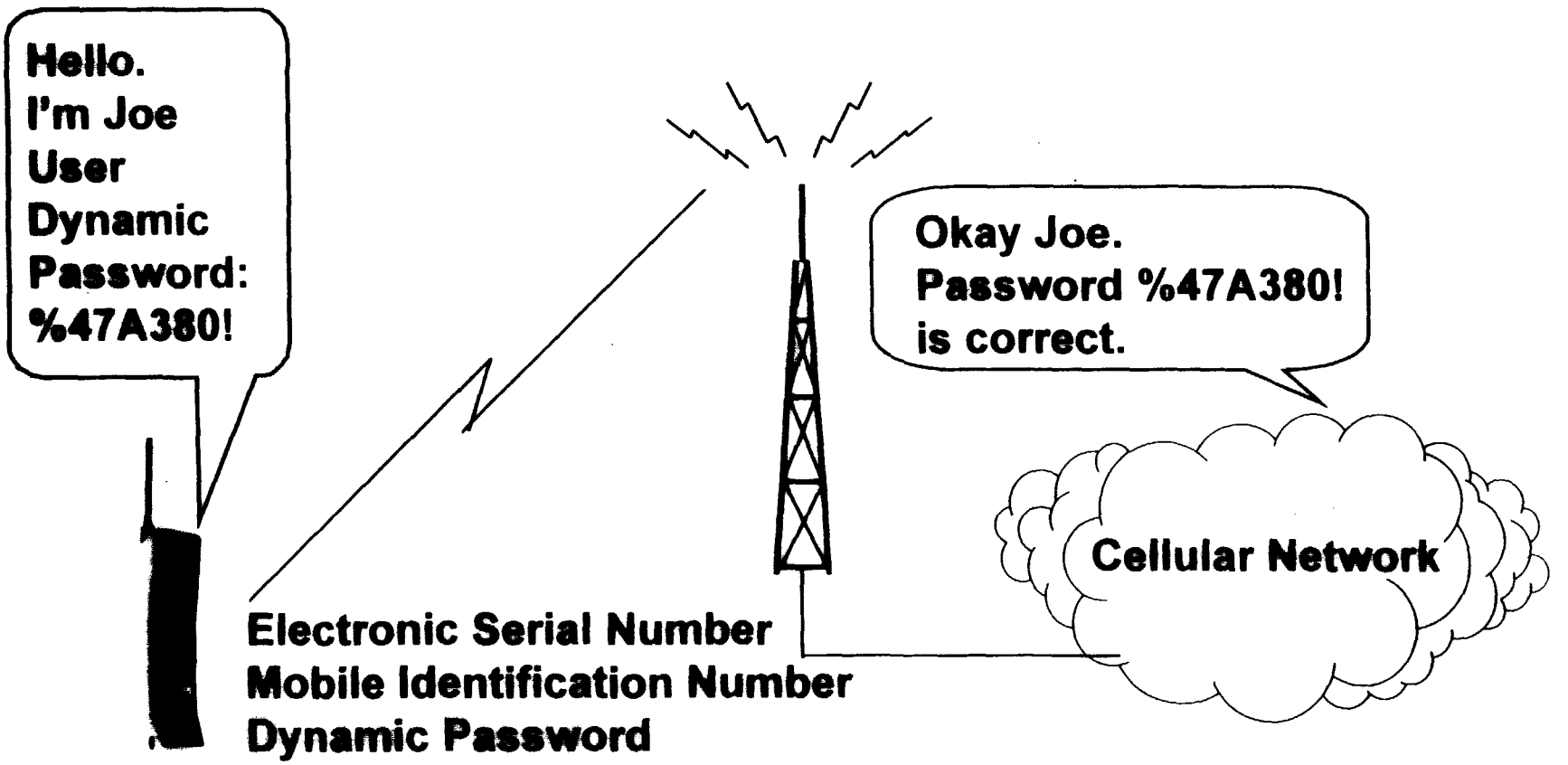
(206) 828-1840 (Office)
(206) 828-2334 (Fax)
les.owens@attws.com (Email)

Agenda

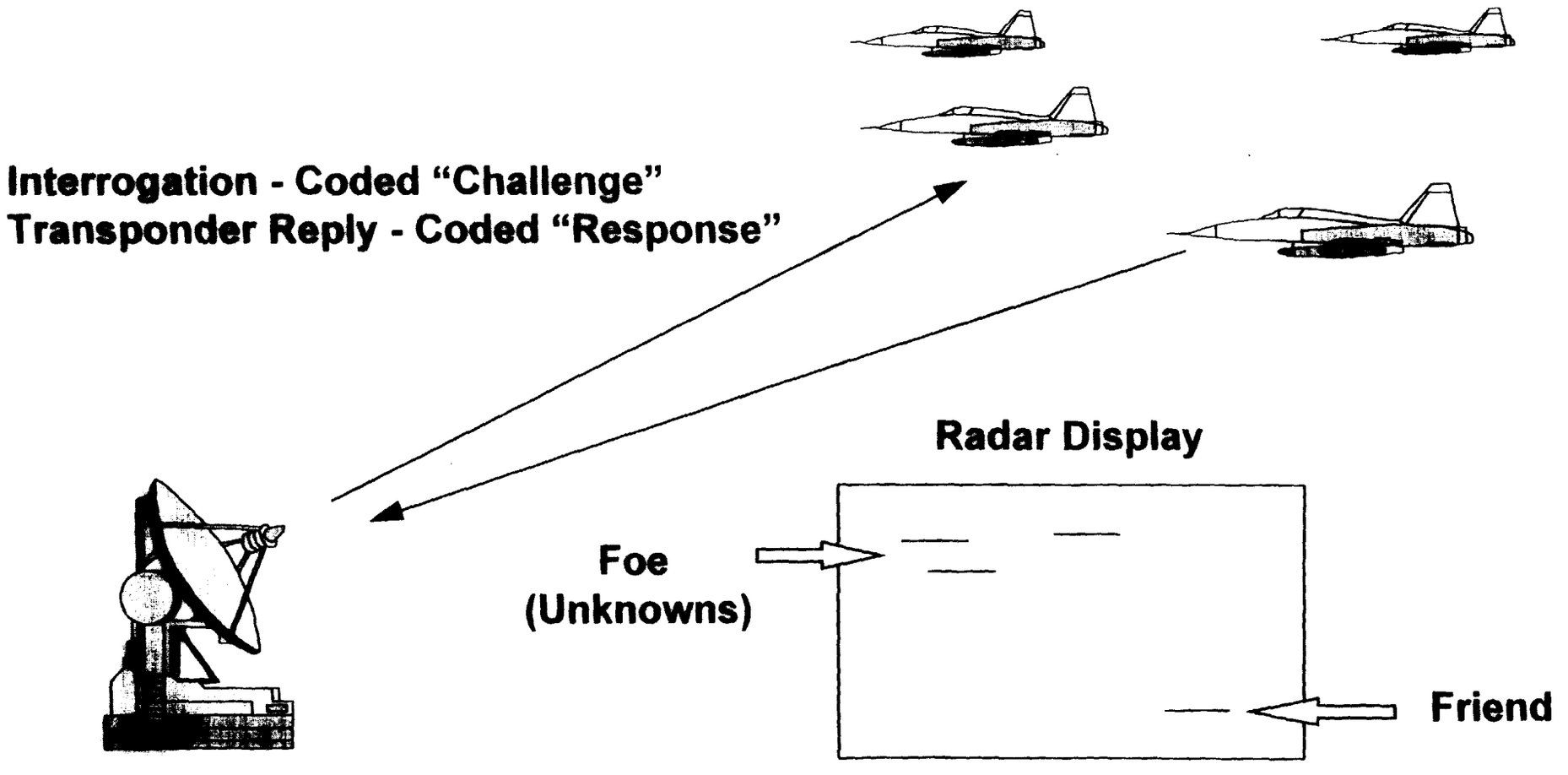


- Status and History of the Cellular Industry and Cellular Fraud
- Cellular Fraud Facts and Trends
- Taxonomy of Fraud and of Counterfeit Telephones
- Techniques and Tools to Combat Fraud
- Introduction to Cryptology and "Challenge-Response" Authentication
- Slideshow of Bandit Tools and Telephones
- Demonstrations

Cellular Challenge-Response "Authentication" Scheme



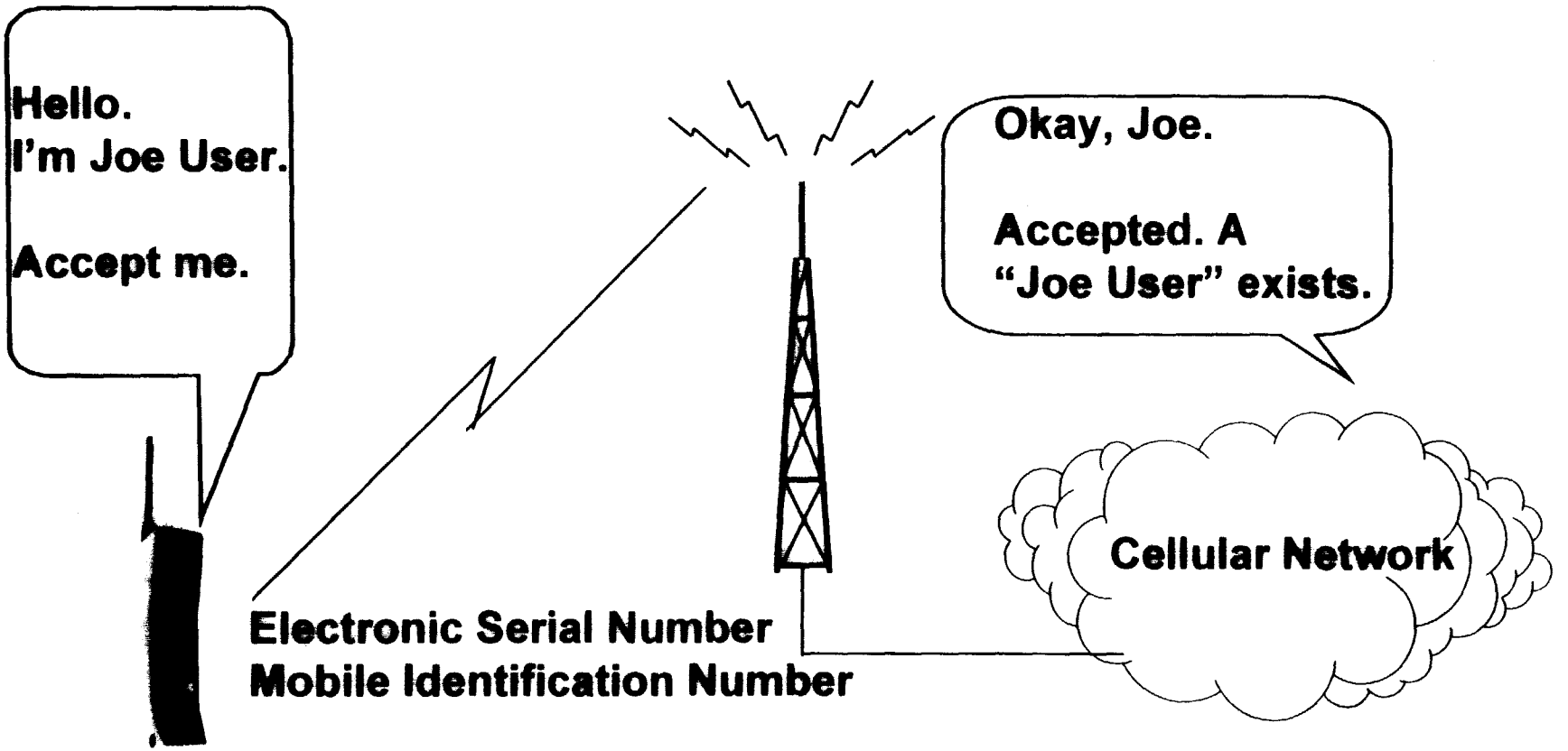
Basic Principles of Identification, Friend, and Foe (IFF)



Fundamental Definitions

- **Identification**
  - **Process whereby the cellular network recognizes a subscriber's identity over the radiopath**
  - **Analogous to a computer *UserID***
- **Authentication**
  - **Process whereby the cellular network verifies the claimed identity of a subscriber to protect the network against unauthorized use (theft of service)**
  - **Analogous to a password associated with the UserID**
  - **In the cellular environment, the password is "dynamic": changing on every access attempt**

Current Cellular "Identification" Scheme



Authentication ... A Closer Look

Money Dispensing at ATM Machine — Everyday Authentication

History of Cryptography

- **Circa. 1900 B.C. — Birth of Cryptology**
  - Egyptians use hieroglyphic symbols to document history
- **50 B.C.**
  - Julius Caesar writes to friend Cicero using the "Caesar alphabet"
- **Middle Ages**
  - Geoffrey Chaucer uses symbol cipher in several works
- **Late 1700's**
  - Thomas Jefferson — the Father of American Cryptography develops "cypher wheel"

History of Cryptography (cont'd)

- **Civil War Period**
  - Armies use "word transposition" cryptography to protect military communications
- **1926**
  - Vernam develops concept of "one-time pad" telegraph cipher
- **World War II Period**
  - U.S. uses Hagelin (Converter M-209) for military communications
- **1974**
  - IBM develops Data Encryption Standard (DES)
- **1995**
  - U.S. introduces authentication for cellular