Study K-500 August 3, 1995

First Supplement to Memorandum 95-34

Admissibility of Electronic Documents

In considering Memorandum 95-34, the following additional points may be of interest to the Commission:

JUDICIAL COUNCIL: COURT TECHNOLOGY ADVISORY COMMITTEE

The Judicial Council has been active in integrating electronic technology in the court system. After a recent task force study, it formed the Court Technology Advisory Committee, a standing advisory committee whose function is to "promote, coordinate, and facilitate acquisition and implementation of information and communication technologies useful and appropriate to the courts." See Rule 1033 of the California Rules of Court; see also *Judicial Council of California: Report of the Court Technology Task Force*, adopted by the Judicial Council on Jan. 25, 1995 (hereafter "*Report of the Court Technology Task Force*").

The *Report of the Court Technology Task Force* (pp. 31-34) identifies "nine critical projects" that the Court Technology Advisory Committee should address "as soon as possible." Notably, none of these projects focuses on the rules of evidence, but some of them may involve analyses that are also applicable in the evidentiary context. For instance, projects such as developing a statewide court information network and experimenting with filing documents electronically will require implementation of security standards such as encryption. *See Report of the Court Technology Task Force*, at A-2 (Goal 1, Point 1.1.7), A-7 (Goal 5, Points 5.1.1, 5.1.6). Encryption technology is also relevant to the evidentiary requirement of authentication: Existing rules of authentication could be supplemented with a new statute stating that a document meeting certain encryption requirements is adequately authenticated.

In view of such potential overlap, or for other reasons, the Court Technology Advisory Committee may consider it unnecessary for the Law Revision Commission to get involved in updating the Evidence Code to accommodate electronic evidence. On the other hand, however, the Commission and the Court

Technology Advisory Committee could perhaps complement one another in this area:

> • By studying the evidentiary rules and recommending changes to accommodate electronic evidence, the Commission may further a goal that the Judicial Council considers desirable but not as pressing as the projects enumerated above.
>
> • In the course of its study, the Commission may benefit from the expertise of the Court Technology Advisory Committee. Additionally, in some contexts the Commission may conclude that the Judicial Council should have statutory authority to establish specific standards of one kind or another (e.g., encryption standards for meeting authentication requirements).

Obviously, it would be helpful to know the Judicial Council's perspective on these points.

EVIDENTIARY PRIVILEGES

As mentioned in Memorandum 95-34, if the Commission undertakes to update the Evidence Code to accommodate electronic evidence, areas of the Code meriting particular attention include the best evidence rule (see Memorandum 95-41), authentication requirements, and the official records and business records exceptions to the hearsay rule. Another major area in which changes to accommodate electronic technology may be in order are the rules establishing evidentiary privileges. The realm of electronic communications raises many privacy issues, as is vividly demonstrated by the recent incident involving widespread electronic distribution of what was intended to be a private message describing the rescue of Scott O'Grady in Bosnia (see Exhibit pp. 1-2).

Many of the privilege rules are so generic that they do not need to be changed to reflect the dramatic rise in electronic communications. But consider, for instance, the following italicized language that was added to Evidence Code Section 952 in 1994:

> 952. As used in this article, "confidential communication between client and lawyer" means information transmitted between a client and his or her lawyer in the course of that relationship and in confidence by a means which, so far as the client is aware, discloses the information to no third persons other than

> those who are present to further the interest of the client in the consultation or those to whom disclosure is reasonably necessary for the transmission of the information or the accomplishment of the purpose for which the lawyer is consulted, and includes a legal opinion formed and the advice given by the lawyer in the course of that relationship. *A communication between a client and his or her lawyer is not deemed lacking in confidentiality solely because the communication is transmitted by facsimile, cellular telephone, or other electronic means between the client and his or her lawyer.*

Even assuming that this amendment sufficiently addresses the privacy issues relating to electronic communications in the lawyer-client context, consider its impact on Evidence Code Sections 980 (privilege for confidential marital communications), 992 (confidential communication between patient and physician), 1012 (confidential communication between patient and psychotherapist), 1032 (penitential communication), 1035.4 (confidential communication between sexual assault counselor and victim), 1037.2 (confidential communication between domestic violence victim and counselor). In varying degrees, those statutes are similar to Section 952 as it existed prior to the 1994 amendment, yet none of them have been amended in similar fashion. To prevent misinterpretations, this lack of consistency should be remedied, or at least examined and explained.

STATUS OF PENDING LEGISLATION

AB 1577 (Bowen). Digital Signatures

AB 1577, formerly the California Digital Signature Act, as amended again in the Senate on July 18, 1995, now pertains only to use of a digital signature in a "written communication with a public entity, as defined in [Government Code] Section 811.2, in which a signature is required or used." See Exhibit pp. 3-4.

SB 1034 (Calderon). Evidence; electronic media

SB 1034 would amend Evidence Code Section 250 and Code of Civil Procedure Section 2031 to facilitate discovery of computer evidence. The current version of the bill includes the following legislative findings regarding computer evidence:

> The Legislature hereby finds and declares all of the following:

(a) That computerized recordkeeping has replaced more burdensome manual recordkeeping systems to the point where businesses and individuals rely primarily, if not exclusively, on computer information in conducting their commercial and personal affairs.

(b) That from the largest corporations to the smallest families, people are using computers to cut costs, improve production, enhance communication, store countless data, and improve capabilities in numerous aspects of human endeavor.

(c) That computers have become so commonplace that many lawsuits involve discovery of some type of computer-stored information.

(d) That the development of new technologies for using, storing, and transmitting information allows parties to test the rules of disclosure or discovery by using these new technologies as a basis for withholding information otherwise falling within the scope of subdivision (a) of Section 2017 of the Code of Civil Procedure.

(e) That it would be a dangerous development in the law if new techniques for easing the use of information become a hindrance to discovery or disclosure in litigation.

(f) That the principle embodied in California's discovery statutes is that information which is stored, used, or transmitted in new forms, including computer data, should be available through discovery with the same openness as traditional forms.

(g) That case law interpreting applicable provisions of the federal Rules of Civil Procedure relating to computer discovery amply illustrate this point.

(h) That the new developments in computer technology require greater clarity in California's discovery statutes to keep pace with these advances.

(i) That plaintiffs and defendants, demanding parties and responding parties, all bear an equal obligation to ensure the responsible use of the discovery process by engaging in good-faith efforts to employ the most efficient means of producing, and utilizing computer-stored information.

The bill, last amended on July 7, 1995, remains pending in the Assembly.

SB 926 (Calderon). Writings; electronic media

SB 926 would clarify that for purposes of the Public Records Act and Evidence Code Section 250, the term "writing" encompasses computer data stored on magnetic media. There has been no legislative action on the bill since mid-March.

ISSUES TO RESOLVE

In sum, the issues before the Commission include:

(1) Does the Commission wish to pursue a study of evidentiary issues relating to electronic evidence?

(2) If so, how would the Commission like to proceed?

(a) Through piecemeal reforms as the need appears (e.g., eliminating the above-described inconsistency regarding evidentiary privileges)

(b) Through a more systematic, comprehensive review of the Evidence Code, which could either:

— track the current organization of the Code, but begin with areas that seem to warrant particular attention (e.g., authentication, privileges, best evidence rule, hearsay rule)

— focus on categories of electronic evidence (e.g., email, facsimiles, Internet sites, electronic evidence generated specifically for litigation) and consider each category in turn

— follow some other approach

(3) If the Commission decides to go forward with a study, should we obtain a consultant? If so, who?

(4) Additionally, if the Commission opts to do a comprehensive study of electronic evidence, it may want to discuss, but need not now decide, whether its general approach would be to:

(a) make the rules of evidence specific, such that they provide precise guidance regarding the various existing technologies

(b) make the rules of evidence fairly generic, such that they accommodate new types of technology without requiring constant amendments

(c) make the rules of evidence fairly generic, but give another organization (e.g., the Judicial Council) authority to promulgate more specific implementing rules, at least in some circumstances.

Respectfully submitted,

Barbara S. Gaal
Staff Counsel

SAN JOSE MERCURY NEWS 7/11/95

Pilot's rescue hits Net in error

■ Bosnia: An airman meant to send the secretive account to friends.

BY BRIGID SCHULTE
Mercury News Washington Bureau

WASHINGTON — It started as a simple electronic high-five among friends. Just hours after the Scott O'Grady rescue in Bosnia, an F-16 fighter pilot, still pumping adrenalin, sat down at his computer and banged out a raw firsthand account of the mission.

"The whole thing from the authentication to the pickup was about 10 minutes (seemed like an eternity). To hear communications like, 'Basher 52, got you in sight,' was pretty moving, especially after thinking for most of the week that Zulu (O'Grady) was a mort (dead)," he wrote.

Then, the pilot, Capt. Scott Zobrist, did what is becoming commonplace in this information age: He hooked up to the commercial Internet and sent the report from his base in Aviano, Italy, to a handful of his Air Force buddies and "other . . . Hot Fighter Gods on the net."

And with the push of a button, his world changed forever.

Zobrist's private message — including digs at the Bosnian Serbs, explicit descriptions of radio frequencies, pilot code names, exact times and weapons loads for the mission — was passed around the world to thousands and then posted on an America Online bulletin board accessible to millions.

See PILOT, Back Page

Pilot's recollection of rescue put on-line

■ PILOT

from Page 1A

From Aviano to Air Force bases in South Korea and Japan and on to friends and to friends of friends, the report, written in salty fighter-jock lingo, spread like a cybereruption. With each forward, the number of people receiving the message exploded exponentially.

There, for all to read was information that O'Grady, at numerous press conferences after his rescue, said he could not answer.

The implication of Zobrist's act for the Pentagon, where controlling information is regarded as a critical war-fighting tool, is staggering.

"(Zobrist's message) was more detailed and more in-depth than what intelligence sources were providing under classified covers," said one chagrined senior Pentagon official last week.

"I think this is probably already well documented in Pyongyang, Beijing, Tehran and anywhere else where they're interested in U.S. air operations," said an angry Major Gen. Edward B. Atkeson, a former intelligence officer now at the Washington-based Center for Strategic and International Studies. "I feel sorry for him. But I feel sorrier for the guys who're going to run the next mission."

If Zobrist had written a letter, phoned his mother or regaled buddies in a bar with tales of the rescue, intelligence experts say he would have violated Pentagon regulations on the release of sensitive information. Still, the story would have died in a few days.

As Zobrist and the Air Force were soon to discover, the rules are different in commercial cyberspace. Nothing is private. Anything goes. And everything happens in the blink of an eye.

"We need to recognize that there is a new paradigm out there for information flow," said Brig. Gen. Ron Sconyers, top Air Force spokesman at the Pentagon. "We need to either control it ourselves or figure out some way to control it. It's growing faster than we can keep up with."

Right now, the rigid hierarchy at the Pentagon isn't quite sure just how to tame the babbling anarchy of cyberspace. Although officials are now drafting a policy to classify e-mail as an official record, there is as yet no guidance on what should or shouldn't go out over private e-mail. All Pentagon computers, however, admonish users not to transfer classified information on unsecured lines.

"More people at the Pentagon are concerned about hackers getting in than about information getting out in cyberspace," said Robert H. Anderson, a computer scientist with the Rand Corp. who works on Pentagon computer security.

Sconyers said he did not think Zobrist, one of an unknown number of active members of the military with private e-mail addresses, would be disciplined. "My guess is, someone will use it as a good bad example," he said.

Zobrist himself declined to be interviewed about the incident. But associates say that perhaps no one is more chagrined about the O'Grady report than the unsuspecting pilot himself.

"(Zobrist) had no intention of that going beyond a few friends," said Capt. John Pope, an Air Force spokesman for the fighter wing in Aviano.

But cyberspace doesn't respect intentions. Kevin Kelly, editor of Wired, a computer magazine, has called the Internet, the global system of interlocking computer networks, "the largest working anarchy in the world."

Normally, any material released to the media by the military has been cleared up and down several chains of command and "sanitized" of all sensitive information and, usually, all color.

What gives the Pentagon heartburn is not only that Zobrist's message bypassed the censors, but that it wasn't officials with security clearances reading it. Everyone else was.

Within minutes of receiving Zobrist's gripping June 8 rescue account, his Air Force friends sent the message to their friends with Internet e-mail addresses, who passed it on to others.

The message zipped around the globe in cyberspace, from Air Force bases in South Korea and Japan to a retired pilot in Australia, who posted it on a worldwide aviation electronic bulletin board available to thousands. From there, it zinged into international defense contracting and software companies and bounced into various chat groups.

Pentagon officials are not the only ones who can't control unfettered cyberspace. The people who run it can't, either.

Lee Ewing, director of content for Military City Online, a popular area on America Online, received Zobrist's powerful account of the O'Grady rescue in his e-mail. He sent Zobrist an electronic message asking for permission to put it on Military City Online.

Zobrist messaged him back and asked him not to, saying he had no idea his account would crisscross the globe and that he feared any further spread would ruin his career. Ewing agreed.

But June 30, a Military City Online subscriber known in cyberspace as TFox 2069 put it out anyway, and suddenly 3 million people had access to it. Ewing doesn't plan to do anything about it.

"It gets a little tricky here. Even though I wouldn't post it myself, unless it's something that's libelous or that violates America Online terms of service, then we don't censor subscribers," Ewing said. "There are a lot of things posted we certainly don't endorse or agree with . . . but we don't remove them just because they're controversial."

Where to read it

The transcript of Zobrist's message is available in the Military City Online section of America Online. Users will find it in the Open Forum under the heading O'Grady's Rescue.

'To all my Viper buds . . . on the net'

Mercury News Washington Bureau

WASHINGTON — Here are excerpts from Air Force Capt. Scott Zobrist's report on the rescue of Scott O'Grady as distributed on the Internet and posted on America Online's Military City Online.

Defense officials acknowledge that the report has been so widely disseminated that further distribution would not cause more damage.

⊏

(8 June 95)

To all my Viper buds and other . . . Hot Fighter Gods on the net

It was a good day at Aviano! As you guys have no doubt heard, we rescued Scott "Zulu" O'Grady today after 6 days . . . in the Bosnian countryside. We had an idea that he was still out there but hadn't had positive radio contact until . . . this morning.

. . . The comm went something like this:

"Basher 52 this is Basher 11" click "Basher 52, this is Basher 11, are you up on this freq?" "This is Basher 52" "Say again, understand this is Basher 52" "This is Basher 52. . . . I'm alive" "Say again, Basher 52, you are weak and unreadable, this is Basher 11" "This is Basher 52"

Pause

"Basher 52, what squadron were you in at Kunsan?" "Juvats! Juvats! I'm alive!" "Copy that, you're alive! Basher 52, sit tight and come back up at 15 past the hour."

T.O. (Capt. T.O. Hanford) then started coordinating . . . to pass words to the Deny Flight CAOC (command center) that he had positive radio contact with Basher 52. They replied that T.O. should pass the word "mañana" to Basher 52.

When he did, Zulu replied "I want to get picked up tonight!" (imagine that). So T.O. passed that to the CAOC and the decision was made to press with a rescue.

. . . The whole thing from the authentication to the pick-up was about 10 minutes (seemed like an eternity). To hear comm like, "Basher 52, got you in sight," was pretty moving, especially after thinking for most of the week that Zulu was a mort. . . . I've never been choked up in the jet before, but I was this morning.

Unfortunately, they weren't out of danger yet. . . . I heard the escort chopper . . . say, "Bud, impacts underneath you. SAMS IN THE AIR! SAMS IN THE AIR!" . . . Luckily, they missed, although they took some small arms fire and apparently the gunner . . . silenced that. About 10 minutes later, we heard the call that they were feet wet, then shortly after that that they had "mother in sight" (the ship), two more bits of comm that I will never forget. . . .

I thought you might enjoy hearing the story straight from the CSAR Commander of VTR Ops! Hope it wasn't too mushy, but after all, I did cry when I watched Old Yeller. That's just the emotional type of guy I am!

. . .

Fly safe. . . . Zobe

AMENDED IN SENATE JULY 18, 1995

AMENDED IN SENATE JUNE 19, 1995

AMENDED IN ASSEMBLY MAY 30, 1995

AMENDED IN ASSEMBLY MAY 15, 1995

AMENDED IN ASSEMBLY MAY 2, 1995

CALIFORNIA LEGISLATURE—1995–96 REGULAR SESSION

ASSEMBLY BILL No. 1577

Introduced by Assembly Member Bowen
(Principal coauthor: Assembly Member Cunneen)

February 24, 1995

An act to add Section 16.5 to the Government Code, relating to digital signatures.

LEGISLATIVE COUNSEL'S DIGEST

AB 1577, as amended, Bowen. Digital signatures.

Existing statutes do not generally govern the authenticity and verification of electronic or similar data intended to act as a signature, except in the case of electronic fund transfers in nonconsumer situations in which case existing law provides for security procedures related to verification of authenticity of orders.

This bill would provide that, in any ~~transaction in which~~ *written communication with* a public entity ~~is a party, at the option of the parties,~~ a signature may be affixed using a digital signature and that in those ~~transactions~~ *communications*, the use of a digital signature would have the same force and effect

as the use of a manual signature. ~~The bill would define a digital signature~~ *if it complies with the bill's requirements*, including a requirement that it conform to regulations adopted by the Secretary of State. *The bill would exempt certain reports relating to environmental protection. The bill would define a digital signature.*

Vote: majority. Appropriation: no. Fiscal committee: yes. State-mandated local program: no.

The people of the State of California do enact as follows:

SECTION 1. Section 16.5 is added to the Government Code, to read:

16.5. (a) In any ~~transaction in which~~ *written communication with* a public entity, as defined in Section 811.2, ~~is a party~~ in which a signature ~~of a party to the transaction is required or used, at the option of the parties, any party to the transaction~~ *is required or used, any party to the communication* may affix a signature by use of a digital signature that complies with the requirements of this section; ~~in which case the~~ *The* use of a digital signature shall have the same force and effect as the use of a manual ~~signature.~~

~~(b) "Digital signature" means an electronic identifier, created by computer, that embodies all of the following~~ *signature if and only if it embodies all of the following* attributes:

(1) It is unique to the person using it.

(2) It is capable of verification.

(3) It is under the sole control of the person using it.

(4) It is linked to data in such a manner that if the data is changed, the digital signature is invalidated.

(5) It conforms to regulations adopted by the Secretary of State. Initial regulations shall be adopted no later than January 1, 1997. *In developing these regulations, the Secretary of State shall seek the advice of public and private entities, including, but not limited to, the California Environmental Protection Agency and the Department of General Services.*

~~(c)~~

(b) The use or acceptance of a digital signature shall be at the option of the parties. Nothing in this section shall require a public entity to use or permit the use of a digital signature.

(c) Digital signatures employed pursuant to Section 71066 of the Public Resources Code are exempted from this section.

(d) "Digital signature" means an electronic identifier, created by computer, intended by the party using it to have the same force and effect as the use of a manual signature.