

Why Not Private Email?

Email permits convenient, casual, even intimate conversations that transcend distance and time. Yet as the White House, Microsoft, and all of the rest of us have learned, email can be treacherous. The sender has no control over his message, and the recipient who fully trusts the “delete” button is a fool. Yet email is on the verge of a revolution. Encryption software now exists that permits the sender to control his message – its lifetime, who can open it, and who can print it, but only up to a point. The technology exists for email users’ machines to negotiate for users a mutually agreeable level of privacy for sensitive messages. The real question is whether the law will catch up with this technology and fulfill our expectation of privacy so that sensitive email is treated as a private conversation, just as with the telephone.

The Promise of Technology

An op-ed from The New York Times of March 26, entitled, “E-Mail Is Treacherous. So Why Do We Keep Trusting It?” by Amy Harmon, outlines the tension between our habit of treating email as if it were private and our painful experience that teaches us the folly of such reliance. Many such articles chasten us for doing what comes naturally – treating email as casual banter around the watercooler, as unrecorded “conversation.” Economists no doubt can quantify how valuable email is in enhancing productivity, but real email privacy would make email even more valuable. The problem is that email creates a record—a pesky record that seems almost indestructible and is therefore the target of any good lawyer’s discovery request. Such records of entirely legal “conversations” inhibit creative brainstorming and often later lead to out-of-context misinterpretations of private exchanges.

Several companies offer software products that enable the sender to encrypt and control the receiver’s access to the message through a key. Once the key expires, the message is unreadable, virtually shredded. For example, QVTech, and appropriately enough, Disappearing Inc., both offer such products. For now, such encryption technology is only as reliable as your partner. While encryption will prevent disclosure to third parties, if the recipient hand-copies the decrypted message from the screen or prints or videotapes the screen, then a record of the conversation will exist, a discoverable record. Nevertheless, for senders and receivers with a mutual interest in preserving the privacy of the communication, such software packages offer a true revolution in email. The email message will carry with it a document retention and email security policy embedded in it that is specified by the sender.

In his book *Code*, Lawrence Lessig describes how email users could rely on their machines to negotiate automatically the level of privacy that a sender and

Wiley Rein & Fielding

receiver agree to practice in their message exchange, e.g. no forwarding, no copies, delete within 30 days. If the other party is unwilling to accept the level of privacy upon which the first party insists, then no communication would ensue. (One could even imagine terms that would include in effect a privacy contract, complete with liquidated damages.) Email could then offer variable privacy.

A Need for Supporting Law

Still, the privacy would be imperfect. True, the message would be unreadable once the encryption key automatically expires. However, if the receiver (or the sender) kept a bootleg copy of the decrypted message, it would still be discoverable, although contractual remedies might result. Even the encrypted message would be discoverable as long as the key is available. Perfect privacy would probably require legislation to afford special protection, a privilege, to encrypted email for which the parties have agreed to a high level of privacy, including an agreement not to keep any records of the “conversation.” The analogy might be laws that recognize privileges for conversations in relationships such as patient-psychiatrist. Such a rule could ensure that our expectation of privacy in sensitive email is not misplaced.

For further information, please contact [James T. Bruce](mailto:jbruce@wrf.com) (202.719.7552 or jbruce@wrf.com).