Date: March 12, 2001

Josephine Scarlett
Office of the Chief Counsel
National Telecommunications and Information
  Administration
Room 4713 HCHB
1401 Constitution Ave., NW
Washington, DC 20230

Re: Docket No. 010222048-1048-01; Request for Comments on Section 105(b) of the Electronic Signatures in Global and National Commerce Act.

Thank you for the opportunity to address the National Telecommunications and Information Administration (NTIA) on the very important topic of technology issues associated with implementation of the Electronic Signatures in Global and National Commerce Act ("ESIGN"). I write as a representative of Yuroka™, a provider of electronic personal authentication services that uses both biometrics and encryption.

The enactment of the ESIGN law is a dramatic development that Yuroka believes can create trust within the public towards electronic commerce. As requested by your notice, these comments will focus on the types of technology being used to ensure the security of transmissions. Through biometrics, the Yuroka system enables a user to consent to the use of electronic signatures and receive proper disclosures as required by law. This comment will also highlight an inconsistency with respect to biometrics within the law that should be addressed.

The Act requires that consumers receive information regarding their right to consent to the use of an electronic signature as well as a means to actually give affirmative consent to its use. Yuroka's authentication technology, that includes voice verification and Interactive Voice Response (IVR), is the perfect tool for consumers to give their consent because consumers are already accustomed to using voice in their daily activities to give instructions. In addition, the infrastructure needed to accommodate voice-based transactions already exists, thereby precluding the need for expensive equipment.

The Yuroka Solution

Yuroka has developed an authentication process that integrates biometrics,[1] a password and a user device. The use of biometrics creates a "one-to-one" relationship between a consumer and his or her individual transaction. We favor the use of biometrics, which especially when coupled with a password and user device, decreases the possibility of fraud in remote transactions. Internet transactions must operate with a high degree of trust that the person on the other end of the connection is whom he or she claims to be.

Unfortunately, criminals may abuse this trust and commit identity theft or illegally access sensitive data. Current security measures like PIN codes or passwords remain insufficient because they are transferable. For example, a digital signature only identifies a computer and not the person who operates it. If a user gives someone your lap top computer, that person would own the digital certificate contained on its hard drive that was supposed to relate to the user.

Enabling ESIGN

The Yuroka solution, using both IVR and a web browser, could provide the consumer with notification that they will be asked to give their consent to the use of an electronic signature. Under the terms of ESIGN, the biometric would function as the signature.

Further, both IVR and Internet could relate any information that the law required the customer to be informed. Further, the system could ask that consumer to state "YES" or "NO" whether they understand their rights.

A positive aspect of speech as a means of communications is that it is user friendly and a reliable means for a person to accept terms. Many would consider it a superior way to accept terms since it is really an affirmative act that would not often occur by mistake as, for example, when a person accidentally clicks the "Accept" button with a mouse too quickly. Further, a voice prompt during the telephone session could force a listener to pay attention and urge the customer to think about whether or no they wish to agree to the terms that will see on their screen.

An Example

The following is an illustration of the Yuroka solution and how its authentication technology can benefit the consumer:[2]

A customer seeks to buy items for her business through the Internet. She accesses the Yuroka web site and clicks on a login URL that generates a unique, one-time only code that appears on the web page. She would then separately dial toll-free number into the Yuroka network.

[1] A biometric is defined as a measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity

[2] The example assumes that a user has already registered herself with the system.

She would hear an IVR voice request that she press a button on a Yuroka user device (called a YuCoder™) she has in her possession and place it next to the mouthpiece of the telephone. The YuCoder is a small device designed to fit onto a key chain or be carried with a pocket or purse.

Upon activation, the device emits an encrypted DTMF code that identifies the device as a legitimate YuCoder to the receiving platform. This "pseudo-random" code prevents an outsider from duplicating the device. It also prevents a recording of a previous emission to masquerade as legitimate one, since the code does not repeat. The code generated is also used to unlock an encrypted file that contains elements of the user's voice pattern previously stored during a registration session.

Once the device is authenticated, the customer enters a four-digit code through the keypad similarly chosen during a registration session. The code locates a file that contains the user's voice elements in template form and allows a one-to-one match between the user and the stored data. A one to one match enables high levels of accuracy because the live voice elements are compared with those known to belong to the customer.

The user is then prompted to speak a password or phrase previously registered with the system. If a match occurs, the customer is authenticated.

It is important to state that the identity of the user is never known to the system. The system only recognizes the data emitted from the YuCoder, the PIN number and the biometric elements given by the customer; They are never tied to a person's real name, address or other identifying data. Further, the data maintained on the system (PIN code, biometric) are encrypted, with the keys to decrypt them held by the user in the YuCoder or by the end destination that uses the product (i.e. the e-commerce vendor).

After authentication, the system then asks the user what sort of transaction she wants to occur. In this instance, she would utter "Internet" or "e-commerce" or the name of the company from whom she makes online purchases. The system would understand the request by voice recognition, defined as the ability of a computer system to understand a human voice and act according to its voice.

The system then asks the customer to speak the one-time code displayed on the screen. Through the code, Yuroka's platform then can locate the computer at which the customer is present. This creates a highly precise link between the YuCoder, the biometric and the computer.

Privacy Concerns

The use of biometrics raises questions directly related to privacy. In order to counter these concerns, and the possibility for wrongdoing, safeguards must be incorporated into biometrics technology as well as any other technology used for digital signatures. Many people fear, rightly so, that the use of a biometric would become a tag or de facto ID card that could link their every electronic activity. Surveys have indicated that public trust in electronic transactions is limited and that security and privacy are important concerns to consumers.

Any biometric system implemented should contain various safeguards to protect the privacy of the system's user. Options include the separation of any databases; the use of a template based on facets of the characteristic, rather than an entire pattern; and, placement of the biometric on a secure platform protected with the strongest level of encryption available.

Yuroka has included these safeguards within its system. Since it operates as a gateway for electronic commerce between customers and businesses, it does not require personal data about the user. Yuroka only requires the anonymous code emitted from the device and voice elements from the anonymous user.

The Further Challenge: Convergence of Voice and the Internet

In the near future, experts predict that access to the Internet, telephone and personal computer will come through one terminal point. Once this occurs, a user could perform multiple voice authentications during a continuous connection without the need for separate phone calls.

In light of this coming convergence, it is ironic that the ESIGN legislation contains an incongruity regarding the use of voice. In Section 101 (c) (6) "Oral Communications," an oral communication is disqualified as an electronic record.

Under this section, it is possible that a voice template given by a user may not be considered a record. Yuroka would ask that this inconsistency be clarified under future regulations.

Again, I think you for the opportunity to provide comments on this important issue.

Very truly yours,

David A. Petti
Director of Privacy & Security Policy
Yuroka
95 Morton Street
New York, NY 10014
email: dpetti@yuroka.com
url: http://www.yuroka.com