wiley

NEWSLETTER

E-SIGN May Involve "Fair Information" Privacy Duties

September 2000

On October 1, 2000, key provisions of the federal Electronic Signatures in Global and National Commerce Act ("E-SIGN") take effect. E-SIGN is intended to give electronic signatures and contracts the same legal standing as paper-based signatures and contracts in a nationally uniform manner, and allows the "record" of a transaction to exist solely in electronic form, rather than on paper stored in file cabinets. While this landmark legislation promises to spur electronic commerce in years to come, relatively little attention has been devoted to the privacy issues and obligations E-SIGN may raise in e-commerce and elsewhere.

Personally Identifiable Information

A number of privacy laws are triggered by the collection, use, retention, or transfer of personally identifiable information ("PII"). At least in the consumer market, both the electronic signature and the electronic records authorized by E-SIGN would appear to involve PII, as could the transactions to which they pertain. Although not mentioned in the E-SIGN Act itself, these facts may create additional privacy law obligations on the part of the e-commerce firm that accepts an electronic signature and stores an electronic record. These obligations may also affect any company that purports to certify that a particular e-signature is associated with a particular individual.

FTC Fair Information Practices

Although much of the relevant law of privacy is still unsettled, the Federal Trade Commission has endorsed what have come to be known as "fair information practices." These practices include obligations to provide notice, consent, access, and security with respect to a consumer's PII. Although, to date, these FTC principles are largely advisory, they form the core of privacy seal programs, have been enacted as part of the Children's Online Privacy Protection Act, and are integral to the Department of Commerce's "safe harbor" approach to satisfying the European Union's Privacy Directive. The Gramm-Leach-Bliley Act extended similar protections to certain financial transactions. Given the high degree of attention to privacy issues this year, some may find it strange that the E-SIGN Act contains no explicit mention of privacy. Interestingly, however, E-SIGN appears to implicate virtually all of the elements of the FTC fair information practices, although in terms somewhat unfamiliar to privacy lawyers.

First, consider the e-signature itself. A business receiving a consumer's e-signature thereby acquires personally identifiable information about the consumer – the name. This name, together with any associated transactional information, becomes PII in the possession of the business. Nothing in the E-SIGN Act, however, requires the business to follow any of the fair information practices – or any other privacy practices – before or after collecting the e-signature. Unless the business is enrolled in a privacy seal program, or the consumer is a child under the age of 13, or the transaction relates to medical or financial matters under the Gramm-Leach-Bliley Act, there likely is no obligation to give notice, obtain consent, provide access, or furnish any particular level of security to that PII.

Similar considerations extend to any company serving as a third-party certification authority in the business of verifying an electronic signature, although privacy issues in this context are likely governed by contract with the consumer. For example, a third-party could have an obligation to preserve the security of any passwords used in verifying an identity.

Second, E-SIGN's electronic record-keeping provisions add another layer of privacy issues, although in this context the fair information practices may, in fact, be satisfied. E-SIGN authorizes contracts to be stored electronically, instead of on paper, in most cases where there exists a legal requirement that a contract relating to a transaction affecting interstate commerce be retained. For example, E-SIGN applies to mortgages, life insurance or automobile purchases, software licensing, contracts to build a new deck, and the switching of long distance telephone companies.

In particular, E-SIGN will allow an electronic record to satisfy a retention requirement so long as two conditions are satisfied. One, the electronic record must accurately reflect the information in the original. Two, the electronic record must remain accessible to all persons who are entitled to access it in a form capable of being accurately reproduced by transmission, printing, or otherwise.

Counterpart E-SIGN Required Disclosures

Of course, such an electronic record will almost certainly, in business-to-consumer transactions, contain personally identifiable information. The E-SIGN Act requires enterprises proposing to do business electronically, rather than on paper, to provide the consumer with certain disclosures, including:

- instructions on how the consumer may obtain a paper record, and whether a fee will be charged; and
- a statement identifying the computer hardware and software required to receive electronic records pertaining to the transaction.

Comparing this language to the FTC's fair information privacy practices yields several observations.

First, the E-SIGN disclosures, in total, may amount to the type of "notice" contemplated by the fair information privacy practices. In fact, E-SIGN may go beyond many legal notice requirements by requiring "clear and conspicuous" notice.

The FTC "consent" criterion is satisfied by E-SIGN's requirement that consumers "opt-in" to doing business electronically. Consumers may also change their mind later. Inasmuch as E-SIGN applies to any electronic record – even if the underlying transaction occurred on paper – it appears in effect to extend the principles of notice and consent to non-electronic transactions.

As for "access," E-SIGN establishes an explicit right of consumers to access a record, going so far as requiring businesses to specify the computer hardware and software needed to access the PII. Moreover, if the business later changes the hardware or software requirements in a manner that "creates a material risk that the consumer will not be able to access or retain a later electronic record," it must offer the consumer, without charge, an opportunity to withdraw consent to electronic notice.

However, there is no obligation for the business to provide access to any other PII in its possession that may be related to the same individual. Interestingly, however, E-SIGN specifically contemplates that the business may be able to charge a fee to the consumer for obtaining a paper copy of the record.

Silence on "Security"

As for the fourth element of the FTC fair information practices – security – E-SIGN is silent. The E-SIGN access requirement itself produces some risk of security breach. E-SIGN does not require any particular level of proof that the party seeking access is, in fact, who he or she purports to be; it only requires that access be available to any entity legally entitled to a copy of the record. Although a duty to take reasonable security precautions may be implied under E-SIGN (insofar as the e-record must be capable of being reproduced), there is no explicit obligation not to disclose it to unrelated third parties. Such an obligation might arise under an applicable state or federal privacy law, however, depending on the nature of the transaction.

In sum, while the E-SIGN Act does not expressly adopt the FTC's fair information privacy principles, it appears to require most of them as a practical matter, at least for document retention as e-records. Moreover, practitioners should bear in mind that E-SIGN may extend privacy requirements to offline transactions where a business wishes to save money by storing records electronically, rather than in file cabinets.