MIAMI VALLEY RISK MANAGEMENT ASSOCIATION

LEGAL UPDATE

STORED COMMUNICATIONS ACT
18 U.S.C.§§ 2701 et. seq.

Since 1986, Title II of the Electronic Communications Privacy Act of 1986, Pub.L. No. 99-508, § 201, 100 Stat. 1848, *codified as amended at* 18 U.S.C. §§ 2701-2711, commonly referred to as the Stored Communications Act (SCA), has authorized the federal government to require internet service providers to disclose the contents of "electronic communication[s]" of their customers in certain circumstances, including by way of an *ex parte* court order. *Id.* § 2703(d). On December 14, 2011, the Sixth Circuit Court of Appeals issued a decision in the case of United States of America v. Steven Warshak, et. al , 631 F.3d 261 which merits review by individuals seeking to obtain e-mails from internet providers as part of a criminal investigation. In its decision, the court held that a subscriber enjoys a reasonable expectation of privacy in the contents of e-mails that are stored with, sent or received through a commercial internet service provider (ISP). "The government may not compel a commercial ISP to turn over the content of a subscriber's e-mail without first obtaining a warrant based on probable cause." It concluded that "[M]oreover, to the extent that the SCA purports to permit the government to obtain such emails, warrantlessly, the SCA is unconstitutional." Id.

More frequently, law enforcement seeks to obtain information regarding one's use of a cell phone. The SCA requires that a provider of electronic communication service or remote computing service can only disclose records or other information pertaining to a subscriber or customer of an electronic communication service or remote computing service (not including the contents of communications) when the governmental entity:

(1) Obtains a warrant using State warrant procedure issued by a court of competent jurisdiction;

(2) Obtains a court order for such disclosure which shall only issue if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. However, such an order shall not be issued if prohibited by the laws of the State in which the order is requested;

(3) Has the consent of the subscriber or customer of such disclosure;

(4) Submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud;

(5) Seeks certain, specific information utilizing an administrative search warrant authorized by Federal or State law or a Federal or State grand jury or trial subpoena.

18 U.S.C. § 2703(c)

The court in this most recent Warshak case discussed an individual's expectation of privacy in the contents of an e-mail. As noted in its decision, the application of the Fourth Amendment depends on whether the person invoking its protection can claim a "legitimate expectation of privacy" that has been invaded by government action. This inquiry normally embraces two questions: first, whether the individual has exhibited an actual (subjective) expectation of privacy; and second, whether his expectation is one that society is prepared to recognize as "reasonable." *Katz v. United States,* 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576. Pp. 2579-2580. As part of its analysis, the court recognized that a bank depositor does not have an expectation of privacy in items such as bank records, checks and deposit slips since the information was voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business. Potentially, a comparable argument could be made for records of cell phone usage. See *United States v. Miller,* 425 U.S. 435, 96 S.Ct. 1619, 48 L.Ed.2d 71. Pp. 2580-2583. (When petitioner voluntarily conveyed numerical information to the phone company and "exposed" that information to its equipment in the normal course of business, he assumed the risk that the company would reveal the information to the police.) Nevertheless, the prudent course of action would be to invoke the state warrant procedure to acquire such information and not rely upon the provision of 18 U.S.C.§ 2701 (d) to obtain a court order based solely upon specific and articulable facts showing that there are reasonable grounds to believe the contents of a wire or electronic communication, or the records or other information pertaining to a subscriber or customer are relevant and material to an ongoing criminal investigation.

Surdyk, Dowd & Turner Co. L.P.A.
March 17, 2011

\law director stored communications act