The Legal Intelligencer
THE OLDEST LAW JOURNAL IN THE UNITED STATES 1843-2012
PHILADELPHIA, TUESDAY, JULY 31, 2012 VOL 245 • NO. 21 An ALM Publication

CRIMINAL LAW

HB 2400 Balances Privacy Interests and Law Enforcement Needs

BY RICHARD Q. HARK
Special to the Legal

Modern communication capabilities have far outpaced legislatively supplied police crime-solving tools. Congress and state legislatures have slowly expanded law enforcement's investigative subpoena and search warrant authority over cellphone and smartphone records. On June 13, when the state House of Representatives referred House Bill 2400 of 2012 to the Senate Judiciary Committee for consideration, it began the process of updating Pennsylvania's Wiretap Act, 18 Pa C.S. §5701, for the first time since 1988.

At the outset, the bill amends the term "oral communication" to eliminate a reasonable expectation of privacy in any oral communication if the conversation could be overheard by another person not included in the conversation and actual or constructive notice of interception may be occurring. The bill augments a "tap and trace device" to include any caller identification device that identifies phone numbers and all subscriber and carrier information. The terms "communication service" and "communication systems" are added and defined, respectively, as a service that provides users the ability to send or receive wire and electronic communications, whether doing business in the commonwealth or not, and their communications delivery and storage component entities.

Section 5704(2)(i) authorizes the police practice of supplanting themselves for a layperson to receive incriminating electronic wire communications. Prior to that, however, law enforcement must legally obtain the device to which the communications are being sent. Once the device is legally obtained, any criminal conduct may be observed, responded to and intercepted without disclosing law enforcement's identity. The amendments do not alter §5704(2)(ii), which requires a designee of the attorney general or county district attorney where the interception is to be initiated to confirm pre-interception consent from the device's recipient.

RICHARD Q. HARK
is a partner of Hark & Hark, a regional law firm specializing in all aspects of federal and state criminal defense.

Section 5704(17) is added to allow for layperson warrantless interception of any wire, electronic or oral communication "if that person is under reasonable suspicion that the intercepted party is committing or has committed a crime of violence or a felony of the first degree" and information regarding the crime may be disclosed in the communications. Any person who possesses knowledge of criminal activity may record any communication from the potential perpetrator without the risk of violating the law. The recorder is not required to advise any person of his or her recording activities and there is no expectation of privacy in those communications. This provision ensures that private emails, texts and recorded phone conversations secured prior to law enforcement involvement in a case, rendering §5704(2)(ii) inapplicable, are admissible in any court in the commonwealth.

The bill amends §5714 to mandate that all electronic communication service providers, in response to court-ordered placement of a trap-and-trace device, allow for features that will determine all subscriber information and carrier identity of the persons calling the intercepted line. Significantly, the bill provides for disclosure of any communication service provider, even if it is not a commonwealth-registered company but operates in the commonwealth.

The heart of the bill is the new §5712.1, which allows for target-specific, probable-cause-supported search warrant applications. A law enforcement officer must verify he or she knows the person involved in the crime, does not possess his or her telephone number(s) and the electronic communication service provider keeps changing. Thereafter, a process will be in place for an investigating agency to emergently investigate all communication service providers for any telephone number(s) in the target's name.

Section 5712.1(b) allows law enforcement to secure supplemental court orders under §5712.1(a) upon satisfying a reduced showing of reasonable suspicion of a target's continued criminal activity. The court shall sign these court orders if the burden is met. This is a higher proof burden than the Stored Communications Act, 18 U.S.C. §2701. There, Congress mandates that magistrates issue the disclosure order "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." HB 2400 maintains the commonwealth's heightened protection of citizens' privacy rights when compared to federal law.

HB 2400 maintains current judicial wiretap application information requirements and maintenance of post-interception records of all targets, their telephone and ISP carriers, the times of interception, the officers involved in the surveillance and the progress of such investigation. Law enforcement must conduct the interceptions from the carriers' physical locations. Entry is solely for installation, maintenance and removal of the interception devices and only within 48 hours of notification to the issuing judge.

Section 5717(a.2) provides civil immunity for any civilian surrender to law enforcement wire, electronic or oral communications or evidence derived therefrom, which may be indicia of a first-degree felony. This provision, when read in conjunction with the new §5721.1(a)(4), expands disclosure and admissibility of layperson-derived evidence if such evidence is legally secured while in any jurisdiction and if that person testifies under oath in any proceeding (grand jury, preliminary hearing or trial) in the commonwealth. This section limits admissibility of nonconsensual interceptions from outside the commonwealth to only those that are secured after judicial authorization upon a showing of probable cause that the target is or will violate any state or federal criminal law.

The 2011 Superior Court decision in *Commonwealth v. Koch,* 39 A.3d 996 (2011), discusses evidentiary foundations and authenticity issues of emails, texts and telephone messages. Sections 5704(17), 5717(a)(2) and 5721.1(a)(4) acknowledge the *Koch* court's admissibility ruling by requiring the recipient of any electronic communication to appear in court and testify as to receipt thereof. If HB 2400 becomes law, counsel must ensure that all proffered electronic evidence comports with the new law, *Koch* and Pennsylvania Rules of Evidence 901(a) and (b)(1).

Section 5761 regarding mobile tracking devices is modified to authorize tracking devices only if the criminal conduct occurs in the jurisdiction of the court issuing the warrant. The legal burden under §5761(c)(4) is increased from reasonable suspicion to probable cause that relevant information to a criminal investigation will be produced. This heightened proof requirement complies with the U.S. Supreme Court decision in *United States v. Jones*, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012), which requires a probable-cause-supported warrant before placement of a GPS tracking device.

The most important aspect of today's wireless communications, recording and disclosure of historical and prospective cell site location information, is addressed by adding the term "mobile communications tracking information" in the definition section and utilized in §§5772 and 5773. This term focuses on antenna towers used, the date, time and length of call, call handoffs, registrations and connection records. This is GPS triangulation evidence that pinpoints historical and real-time subscriber location within 50 feet of where a cellphone call was made or received or smartphone Internet usage triggered.

Legislative continuation of our commonwealth's historical preservation of its citizens' privacy and liberty interests is significant.

The vast majority of people in the commonwealth voluntarily carry a GPS tracking device — their cellphones — to which the 2010 SCA amendments gave the federal government almost unfettered access. HB 2400 is more restrictive of the commonwealth's citizens' GPS data. Sections 5772 and 5773 appropriately adhere to a probable cause standard of review in contrast to 18 U.S.C. §2703(d), which mandated access only upon proof of "specific and articulable facts showing that there are reasonable grounds to believe ... the information sought is relevant and material to an ongoing criminal investigation."

Legislative continuation of our commonwealth's historical preservation of its citizens' privacy and liberty interests is significant. HB 2400 appropriately balances the needs for updated criminal investigative techniques with proper judicial oversight of law enforcement. Maintaining a probable cause standard of review and not conceding to a lower proof burden is significant and will not inhibit police investigations. Target-specific warrants address the multi-cellphone user. Allowing for admissibility of previously-illegal, surreptitiously-recorded telephone conversations involving felonious criminal conduct evenly balances the scales of justice.

The age-old evidentiary adage — "You are not protected from your own big mouth" — is now expanded in our digital age to include all telephone conversations, texts and emails. Anyone may now conduct surveillance of someone with whom they converse and are concerned is engaging in felonious criminal conduct. •