Court discusses Fourth Amendment in digital age

By Adam J. Sheppard

In George Orwell's haunting classic, "1984," he wrote of a world where "technological progress only happens when its products can in some way be used for the diminution of human liberty." Today, many of the technologies we cherish, from smartphones to GPS systems, also have the capacity to eviscerate our privacy. Has Fourth Amendment jurisprudence kept pace with these new technologies? This article summarizes recent developments in the area of GPS monitoring, cellphone searches and e-mail searches.

GPS monitoring is a significant privacy issue. It has the capacity to reveal an "intimate picture" of a person's life *United States v. Maynard*. 615 F.3d 544, 562 (D.C. Cir. 2010). For example, GPS data could disclose "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on." *Jones v. United States*. 2012 WL 171117, *9 (Jan. 23, 2012) (Sotomayor, J., concurring) (quoting, *People v. Weaver*. 12 N. Y. 3d 433, 441–442, 909 N. E. 2d 1195, 1199 (2009)).

On Jan. 23, in *Jones v. United States*, 2012 WL 171117, the U.S. Supreme Court unanimously affirmed a judgment by the U.S. Court of Appeals for the District of Columbia Circuit that held that the government's warrantless installation of a GPS device on a vehicle, and its use of that device to subsequently monitor the vehicle's movements for a four-week period, constituted a Fourth Amendment violation. At Jones' drug conspiracy trial, the government introduced the GPS-derived location data which connected Jones to the alleged conspirators' stash house. Jones was convicted by a jury and sentenced to life imprisonment. The circuit court reversed the conviction, holding that the warrantless use of the GPS device was a Fourth Amendment violation and that evidence obtained pursuant thereto should have been excluded from trial. The Supreme Court, in an opinion written by Justice Antonin G. Scalia, affirmed the appeals court judgment.

The Supreme Court's opinion in *Jones* also has implications for cell site location data technology. Cell site location data discloses "the date, time, called number and location of the telephone when the call was made." *In re Application of the United States for Historic Cell Site Data*, No. H-11-221 (S.D. Tex. Nov. 11, 2011). Lower courts have generally held that law enforcement agents need a tracking device warrant, issued upon probable cause, to engage in cellphone tracking. See id; see also *In re Application of U.S. for an Order Authorizing Disclosure of Location Information of Specified Wireless Telephone*, 2011 WL 3423370 (D. MD. 2011). *Jones* indicates that the Supreme Court would likely rule the same.

Lower courts have also recognized that individuals have a reasonable expectation of privacy in their text messages which is protected by the Fourth Amendment. See, e.g., *United States v. Zavala*. 541 F.3d 562, 577 (5th Cir.2008); *State v. Smith*. 2009 Ohio 6426, 124 Ohio St.3d 163, 920 N.E.2d 949 (2009), cert. den. 131 S. Ct. 102 (2010). The Supreme Court has yet to squarely decide this issue. However, in *City of Ontario, Cal v. Quon*, 130 S. Ct. 2619, 2628-29 (2010), the court did "assume" that an employee had a reasonable expectation of privacy in text messages that he sent and received on employer-issued pager device. (The court did not expressly decide that issue because it was able to dispose of the case on narrower grounds).

One exception to the warrant requirement which courts have routinely applied in the area of text message searches is the search-incident-to-arrest-exception. See *United States v. Finley*. 477 F.3d 250, 259 (5th Cir. 2007); *United States v. Arellano*. 410 Fed. Appx. 603 (4th Cir. 2011). The search incident exception allows officers who make a lawful custodial arrest to conduct a warrantless search of an arrestee's person or the area within the arrestee's reach. Officers conducting a search-incident-to-arrest are permitted to search for evidence relating to the crime of arrest. Courts have reasoned that a cellphone is likely to contain evidence relating to a drug offense and, therefore, a cellphone may be searched incident to an arrest for a drug offense. See e.g., *People v. Nottoli*. 199 Cal. App. 4th 531, 130 Cal. Rptr. 3d 884 (6th Dist. 2011); *Hawkins v. State*. 307 Ga. App. 253, 704 S.E.2d 886 (2010).

With respect to e-mail searches, the government needs a warrant, issued upon probable cause, to obtain e-mails directly from a person's Internet service provider (ISP). See *United States v. Warshak* (*Warshak III*) 631 F.3d 266 (6th Cir. 2010). Whether officers would need a warrant to search e-mails on a cellphone they seize directly from a person or from their home is a closer question. Lower court opinions indicate that Fourth Amendment protections would apply in that scenario. See e.g., *Zavala*, 541 F.3d at 567 ("A cellphone is similar to a personal computer that is carried on one's person; *Finley* indicates that mere possession of a cellphone gives rise to a reasonable expectation of privacy regarding its contents.").

Another salient issue is whether a search warrant for a computer authorizes a search for the e-mails contained in it. A warrant to search a computer does not justify a "general rummaging" through all information on the computer. See *In re Search of 3817 W. West End, First Floor, Chicago, Illinois. 60601*,321 F.Supp.2d 953, 959 (N.D.Ill.,2004); *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162 (9th Cir. 2010). However, if the search warrant describes with particularity the information to be seized — e.g., communications with a specific person — and it is reasonable for officers to believe that such information would be contained in certain e-mails, then a court will likely hold that those e-mails fall within the scope of the search warrant. See e.g. *United States v. Adjani*. 452 F.3d 1140 (9th Cir. 2006); see also *United States v Mann*. 592 F.3d 779 (7th Cir. 2010)).

Fourth Amendment jurisprudence is continually being challenged to "keep pace with the inexorable march of technological progress … " *Warshak III* 631 F.3d at 285. Recent developments in Fourth Amendment law, such as the Supreme Court's decision in *Jones*, signal that courts may be up to the task. It is incumbent on Fourth Amendment advocates to continually press courts to expand the contours of Fourth Amendment protections in the digital age.

Adam J. Sheppard is a partner in Sheppard Law Firm P.C., a criminal defense firm. Sheppard is co-editor-in-chief of the Young Lawyers Journal in the CBA Record. He also serves on the CBA Young Lawyers Executive Council in that capacity.