NEWS RELEASE

Contact: Jim Ormond
212-626-0505
ormond@acm.org

USACM Comments on Carpenter Cell Phone Case before US Supreme Court

US Policy Arm of World's Leading Computing Organization Outlines Concerns about How Technological Advances May Endanger Fourth and Fifth Amendment Rights

NEW YORK, NY, November 28, 2017 – On Wednesday, the Supreme Court will hear arguments addressing a cutting-edge case that is at the intersection of information technology and civil liberties. In *Carpenter v. United States*, the Court will decide whether the Constitution requires that the government obtain a warrant in order to seize records revealing historical locations and movements of cell phone users. USACM, the U.S. Public Policy Council of the Association for Computing Machinery, the world's largest computing professional society, considers this a watershed moment. At issue is the legality of potentially indiscriminate government surveillance.

In modern society, third parties—whether they are phone companies, search engines, social networking companies, hospitals, or even companies that make fitness bands or thermostats—collect and maintain massive amounts of data about people both directly and incidentally, data which can effectively reveal almost everything about individuals. The government's position is that the records are in the hands of third parties—cellular communication providers—and, historically, individuals have had no privacy interest in records maintained by such third parties.

At the crux of this dispute is the recognition that society has changed. Information and communication services, and the infrastructure that supports them, are now ubiquitous. Their use is no longer "voluntary," in the sense that no individual can participate in normal society without making use of such services, whether in the commercial, professional, or personal arenas. This is coupled with the ability of companies to maintain massive databases concerning such usage, and the ability of the government to easily correlate and cross reference such databases—all made possible by recent and rapid advances in information technology. The concern goes beyond mere cell phone records, to all activities of all individuals. And these advances continue.

Until recently, the freedom of the individual from government intrusion was protected not only by law but by the practical difficulties in accumulating and analyzing data. Pervasive data collection, analytics, and other computing technologies are ripping away this practical protection. As a result, the Fourth Amendment's prohibition against unreasonable government intrusion, as well as the Fifth Amendment's guarantee of liberty against government intimidation, are both in jeopardy.

What does "unreasonable" mean if the law permits a technological means to easily do what had once been effectively undoable, and thus viewed as unreasonable when the Fourth Amendment was drafted

and interpreted? At what point does the technological justification for intruding upon the individual, and thus infringing upon rights to be free from surveillance and intimidation, come to an end—or does it continue unabated until these rights become *de facto* meaningless while their shells remain enshrined *de jure*? We must distinguish between the government's legitimate needs—supported by a warrant and probable cause—to obtain the location of a specific suspect, and the government's ability without such a warrant to know the location at any time of any person using a cell phone, a smart vehicle, or a Fitbit.

The issue is not whether such records are obtainable by the government—they are. The issue is whether the government must first obtain a search warrant from a court, based upon probable cause that a crime occurred and that the record to be seized will lead to the perpetrator. Do the Fourth Amendment's requirements apply to computer data focused on an individual and held by a third party? The Court must hold that they do. To do otherwise will enable intrusion into personal lives without oversight by the courts, something rejected when the Bill of Rights was enacted more than two centuries ago.

The classical interpretation of the Fourth Amendment—previously viable—is now at odds with the realities of modern society. Its interpretation must be brought into the current era; the alternative is that the Fourth Amendment, and the liberty interests found in the Fifth, will be rendered meaningless. As more personal information—and more sensitive information—is held by third parties, we must restore the historical balance protecting both the liberty of the individual and the interests of the government.

About USACM

The **ACM US Public Policy Council (USACM)** serves as the focal point for ACM's interaction with the US government in all matters of US public policy related to information technology. ACM US Public Policy Council statements represent the views of the Council and do not necessarily represent the views of the Association.

About ACM

ACM, the Association for Computing Machinery, is the world's largest educational and scientific computing society, uniting computing educators, researchers and professionals to inspire dialogue, share resources and address the field's challenges. ACM strengthens the computing profession's collective voice through strong leadership, promotion of the highest standards, and recognition of technical excellence. ACM supports the professional growth of its members by providing opportunities for life-long learning, career development, and professional networking.

# # #