Statement of Condemnation of U.S. Mass-Surveillance Programs, and a Reminder of Our Ethical Responsibilities as Computer Scientists

We have all been hearing about the NSA's mass-surveillance programs, which go by names like PRISM, BULLRUN, Boundless Informant, and X-Keyscore. The extent of these systems, and of corporate cooperation in U.S. mass-surveillance efforts, have been made public due to disclosures by whistle-blowers like William Binney, Mark Klein, and Edward Snowden, and by authors/journalists like James Bamford, Siobhan Gorman, and Glenn Greenwald.

As a scientist who has spent his career studying *cryptography*—the "mathematical" study of privacy and security—I herein condemn and assert my repugnance of the USA's mass-surveillance programs, and those of all other countries. Mass-surveillance is intimidating, abuse-prone, and anti-democratic. It is likely to engender a dystopian future. I assert that:

- Surveillance data should be collected only on specific targets and for specific cause; entire populations should never be surveilled.
- It is contrary to the ethical obligations of cryptographers, computer scientists, and engineers to participate in the development of technologies for mass surveillance. It is also a violation of professional codes of conduct.
- It is contrary to corporate responsibility for a company to develop, sell, or support artifacts, such as server farms, routers, or analytic engines, intended for mass surveillance.
- Cryptographic protections must never be intentionally subverted by bulk provisioning of private keys or plaintexts to any authority. If such compromise is ordered by a court, users must be informed. If the court order forbids disclosure, it lacks ethical legitimacy.
- Automated means of mass surveillance, including methods enabled by advances in data mining, big data, natural-language processing, and machine learning, are at least as dangerous as headphones and binoculars. A communication is intercepted when it is stored or algorithmically processed for any intelligence purpose, not when it is monitored by a human.

Both US-persons and non-US-persons have a right to be free of routinized surveillance. This right does not spring solely from the US Fourth Amendment; it is a human and natural right as well.

Phillip Rogaway
August 30, 2013
Updated September 9, 2013

The author is a professor of Computer Science at the University of California, Davis, USA.