

Security Versus Privacy

Americans were shocked this past June when Edward Snowden, a previously unknown U.S. security contractor, announced that the U.S. National Security Agency (NSA) was collecting millions of private communications – emails, texts, and telephone records – from thousands of unsuspecting U.S. citizens each day. Snowden leaked top-secret documents to *The Washington Post* and *The Guardian*, a London based newspaper, in support of his shocking allegations.¹ The records collected (referred to as “metadata”) were not the overseas communications authorized for collection by the 2001 U.S. Patriot Act or Patriot Extension Act of 2011 but, according to Snowden, were the daily communications of ordinary U.S. citizens with friends, families, employers, co-workers, and even romantic interests here in the United States. Snowden shocked the American public even further by claiming that he could easily tap into any private email – including President Barak Obama’s – without having to demonstrate probable cause or even obtaining a warrant.²

Reactions in the United States were strong, immediate, and mixed. Some hailed Snowden as a “hero” and “whistleblower” who willingly sacrificed himself to ensure Americans knew the truth about their government. Others, however, reviled Snowden as an “opportunistic traitor,” claiming that a “real hero” would have hired U.S. attorneys and then made his revelations to U.S. Congressional representatives rather than fleeing to nations with historically strained U.S. relationships. Snowden fled from Hawaii, where he had been living, to Hong Kong a month before the allegations were made public; he subsequently fled to Moscow where he has received temporary political asylum. The Department of Justice is now asking for Snowden’s return in order to prosecute him for violations of the Espionage Act.

As inquiries continue, the Director of National Intelligence, James Clapper, sent a written apology to Congress for what he termed a “clearly erroneous” statement, he had given under oath, March 12, 2013. During his testimony Clapper denied the existence of any metadata collection on U.S. citizens. His denial was false.³ Shortly after, Thomas Drake, a former NSA senior executive, stated that certain parts of the government “have become a criminal enterprise” and Snowden’s only option “was to escape the United States of America.”⁴

STUDY QUESTIONS

1. Is it ethical for government employees to reveal classified information entrusted to them?
2. Is it ethical for government agencies to collect private communication records between U.S. citizens?

¹ <http://www.usatoday.com/story/news/2013/07/26/edward-snowden-fbi-russia-nsa/2589319/>

² <http://www.thedailybeast.com/articles/2013/06/12/former-nsa-director-michael-hayden-responds-to-edward-snowden-claim.html>

³ <http://www.foxnews.com/politics/2013/07/03/dni-chief-clapper-apologizes-for-erroneous-answer-on-nsa-surveillance/>

⁴ <http://www.usnews.com/news/blogs/washington-whispers/2013/07/25/nsa-whistle-blowers-defend-snowdens-decision-to-flee>

