1949: Director of Intelligence to his men:
The struggle against Communism is on… there are Americans who are plotting to subvert our government and destroy our freedom. Here is your assignment: Develop ways for this agency to make every individual or group visible to us. I want to know what people read, write, say; I want to be able to know the information that they access, the people with whom they communicate, and the places that they go; I want to have a comprehensive view of all their financial transactions: where their money comes from, what they buy, stocks they trade, the people and institutions that receive their money; I want to know where they live, who they love, what they do, as soon as they do it. We should be able to store a record of every surveillance target that is more accurate and more complete than that possessed by the person we have targeted. Finally, I don't want this information to be something that takes hours, days, months or years to reconstruct: your assignment is to gather this information in real time. Then we will have the knowledge and control necessary to protect our national security.

2014: Report to the Director of Intelligence:
In composing this report, our Committee on National Security reviewed the major directives given the FBI, CIA, and NSA since the beginning of the Cold War in 1949. We are happy to report that our agencies have made strides in achieving the goals set out by the first director in 1949. Much has changed since that time: national and world populations and nonhuman assets have increased the scale of our responsibilities; the movement from the struggle to contain communism to the war on terror has changed the nature of the threat and our tactics; and, of course, the sheer quantity of communication has increased exponentially. It is not just humans but also nonhumans (e.g. sensors, computers) that communicate. At the same time, we have been blest by an epochal event in the history of surveillance: the invention and penetration of the globe by the Internet. What began as a computer science experiment to share valuable mainframe time has now interlinked literally billions of humans and machines on planet Earth. We not only have computer access to most financial transactions nearly as quickly as they happen. We can use GPS to track the movement of cars and cellphone users; we can hack email, browser histories, and social media to investigate the most private facets of our citizens' lives, which they cheerfully put on line for the sheer fun of sharing it! Even when media users are not on-line, improved face and voice recognition software, which are linked to public cameras and phones, along with covert remote activation of the microphones found on most smart phones, have allowed our agencies to track our targets with ease. The world has become almost entirely transparent to us. Of course there are still sources of opacity and friction that complicate our efforts: the legal system, congressional oversight and dangerous new privacy laws, which luckily been more of a problem abroad than in this country. When Congressional oversight committees ask why we need access to corporate records, we talk about international theft of our American innovations; when they ask why we need access to all personal computers, we talk about threats to copyright or the danger of child pornography. However, two groups have proven most resistant to our surveillance programs' goal of total information awareness. Firstly, both old people and back-to-the land types have been slow to

adopt the new technologies that serve as our information portals. Secondly, the terrorists who would do us wrong have proven remarkable capable at eluding surveillance by diverting communications through the use of call centers, couriers, and even outdated analog media. We suspect that there are terror groups communicating by handwriting on paper!

In closing this report, the Committee felt it incumbent upon us to report two very challenging developments. First, since our own information is gathered in large databases, it is highly vulnerable to sudden release. There have emerged dangerous free speech and open access vigilantes who seek instant fame by releasing large datasets of highly sensitive government information. We are using every resource of the law against these individuals, but at times foreign governments, and even some of our own nationals, who view these data pirates as heroes, seek to thwart us. A second problem: since the vast majority of our surveillance builds upon computable information systems which, to be effective, must be linked to the Internet, we have been unable to prevent an alarming increase in successful hacks of our own systems. This has allowed enemy hackers—we suspect the Chinese—to track our surveillance efforts and even gain access to our own surveillance records. We were not even sure how to keep this report a secret. That is why we had it typed by one of the older women in the pool on an IBM Selectric we found in storage. We are not sure what the best way is to respond to this challenge.