The framers of the Constitution designed the Fourth Amendment to protect the citizen’s right to privacy. Specifically, the amendment shelters “persons, houses, papers, and effects” against unwarranted search and seizure (22). While the founding fathers could not have anticipated many of the digital and cyber security issues we face today, previous Supreme Court Justice Harlan outlines the requirements necessary for specific digital concepts to be protected by this amendment. In his concurring opinion on *Katz v. United States (1967)* Justice Harlan says that Fourth Amendment protection necessitates an individual “expectation of privacy” that aligns with a societal recognition that the expectation is reasonable (1967).

Even Justice Harlan could not anticipate specific cyber liberty concerns like the protection of electronic mail. Though he could not have anticipated it, we believe that would agree that the government should not be able to read any citizen’s emails even if they are older than 180 days. E-mail is just like regular mail, but obviously electronic and more efficient with the addition of a password for privacy, which Harlan also mentions. A password serves as a digital lock which is similar to the lock found on a citizen’s house to maintain privacy. Because of the inclusion of a password in all email services, an individual expectation of privacy is created and upheld by society. Why should the government be able to read old e-mails if they are protected by a password, but not be able to read regular mail? A citizen’s mail is private, and tampering with it is a federal offense. We believe electronic mail should be granted the same protection. The fourth amendment states that someone’s papers are protected against unreasonable search and seizures. Your e-mail is essentially your electronic paper, so your email should be protected under the fourth amendment.

In addition to respecting a citizen’s privacy within emails, the government should not be able to track any individual utilizing any Global Positioning System. This is a complete invasion of privacy because an individual’s location should be his or her own personal information. A police tail is very different; when law enforcement follow an individual, that person’s location is not known at all times. With GPS tracking, the police can continually monitor someone’s location. Moreover, most GPS devices require a password; therefore, the expectation and recognition of privacy is inherent in the device. Because of this, the federal government must have a warrant to monitor an individual using GPS. If GPS monitoring without a warrant is legal, then it suggests that the American government has complete control over a citizen’s personal life by supporting the creation of a big-brother state.