The IoT is the general term for how the internet has, and is, connecting various “things,” both object-to-object and person-to-object communications. It can more broadly be defined as the interconnected network of various physical objects which are enabled to send and receive data. The initial popularization of IoT began in the late 1990s and early 2000s. It was popularized by the idea of connecting home appliances to the internet. The term itself was first popularized by Kevin Aston. In 1999, Aston was the executive director of the Auto-ID center at Procter and Gamble (Corcoran, 2016). Aston made the term the title of a presentation that linked the idea of RFIDs within P&G’s supply chain. In the same year, Neil Gershenfield spoke about the principles of the IoT in his book When Things Start to Think (Madakam et al, 2015). The following year, 2000, LG announced the plans for the first Internet refrigerator. For the next few years, several more devices with RFID chips began development. The development of these devices quickly expanded to everyday consumers.

The consumer use of the IoT has grown to such a large scale that most people interact with it daily. It has spread from smart refrigerators, thermostats, phones, vehicles, sensors, and a vast amount of other consumer goods and products (Chapin et al, 2015). [INSERT IMAGE HERE] The IoT has transformed how people live and communicate with various devices. It has unified almost all devices within our grasp, which has led to a great deal of personal control, as well as an abundant amount of individual and group data. There were over 10 billion active devices in the IoT in 2021 and it is estimated that, “there will be 152,200 IoT devices connecting to the internet per minute,” by 2025 (Jovanovic). With the increased number of devices connecting to the internet, by 2025, the data generated is expected to reach 73.1 zettabytes (Jovanovic).

As the IoT continues to grow at such a large scale, a concern for security and surveillance has erupted. Another significant concern of the integration and exponential growth of the IoT is that the data that is being collected may be closely related to people as well as their daily activities and the increased relationships between the ‘digital’ and ‘real’ worlds (Baldini et al.). The vast amount of data that is being generated and shared between devices create ethical concerns regarding the collection and use of data. Thus, new legal and development policies and challenges continue to appear.

A great example of ethical and security concerns around the growth of the IoT can be seen through what happened with Edward Snowden. Snowden worked for the Central Intelligence Agency (CIA) for three years before going to the National Security Agency (NSA) as an intelligence contractor. While working at the NSA, Snowden began to collect information on a secret surveillance program that the NSA was conducting. [ADD MORE ABOUT SNOWDEN]

As these challenges continue to emerge, it is clear that the IoT has become a complex and intertwined web of network connections. With how closely these “things” are communicating with one another, it is important to understand the risks and rewards of how the data is being shared, whether it is public or private, and how secure it truly is. [ADD KEY CONTRIBUTIONS]