**Background**

A major ethical issue in the collection and management of consumer information is the privacy of that information (Bloom, Milne, and Adler 1994; Chonko 1995; Foxman and Kilcoyne 1993; Jones 1991). Internet Privacy also known as online privacy refers to the vast range of technologies, protocols and concepts related to giving individual users or other parties more privacy protections in their use of the global internet. Internet Privacy takes many forms, including mandatory privacy statements on websites, data sharing controls, data transparency initiatives and more. Internet Privacy and anonymity are paramount to users, especially as e-commerce continues to gain traction. Privacy violations and threat risks are standard considerations for any website under development.

One of the biggest things that people talk about when they discuss Internet privacy is the regulation of handling user data. A most commonly cited example is the General Data Protection Rule or GDPR, which is a European standard recently adopted to protect the data of European citizens. Apparently, the act governs data belonging to EU citizens, but the way that the regulation plays out affects many companies in other parts of the world. A multinational company utilizing the global internet (or just a company with international reach) may have any number of European users as members, subscribers or customers. This requires the company to keep GDPR compliance for the corresponding data set. In addition, other countries, states and provinces have come up with their own data privacy laws. Many of these are very much in the nature of trying to close barn doors already opened by a lack of universal internet regulation from the infancy of the World Wide Web itself.

Many kinds of internet privacy technologies and security implementations rely on biometrics as a key method of user authentication. The general idea is that if data is biometrically protected, only the individual with said biometric data has access to it. Early biometric designs included thumbprint and retina scan devices but many of these were not very feasible due to hardware requirements and integrations needed. Now, the promise of voice-based authentication adds a key functionality to internet privacy technology. Many types of data sets can be stored behind a voice-based authentication system, ensuring that only the individual with access will be able to view them.

The way that we use the internet related to our internet privacy is changing rapidly. Now, major technology companies have put in place stricter compliance protocols to increase individual user privacy. At the same time, many privacy advocates are calling for more transparency in how third-party data is used, whether that’s entirely demographic or involving data sets with personal identifiers. At the same time, others are also suggesting that individuals should own data and be paid to sell that data to third parties, which could also add needed transparency to the process. The use of blockchain has been explored as a means of building this new type of privacy compliance. In general, having data sets on a blockchain allows for a more diverse set of capabilities related to manipulating and evaluating that data or keeping track of who has access or where the data is stored. The conversation around internet privacy continues to evolve. New types of professionals and analysts are adopting new concepts and strategies for handling internet privacy as the internet matures and cloud services port ever more sophisticated data sets through global internet trajectories.