Weekly Write Up #3

The power of digital technology has changed the way we communicate. It’s easier than ever to send a simple message across the world and get a reply instantly. At times, the content of what we send to people can vary. Sometimes, it’s something we wouldn’t mind being shared to the public, but other times, the messages we send people could be really sensitive and we wouldn’t want that information to be snooped on. Facebook, the company that owns Instagram and WhatsApp, has a plan to integrate all three of its messaging platforms together. In theory, users would be able to message each other from any of the three platforms. On top of that, all messages would be end-to-end encrypted. This is a major deal because on average 1.5 billion people use Facebook daily, another 1.5 billion people use WhatsApp daily, and at least 500 million people use Instagram daily (Snider, 2019). That’s huge: 3.5 billion people would be using messaging platforms controlled by one company if this plan were to be enacted. That’s half the world’s population using messaging services with end-to-end encryption.

There are some major concerns regarding this plan: a single company (one with a history of privacy issues) now having access to half the world’s communications. Some people see this as a danger and a pathway for Facebook to further its monopoly on communication. But the bigger issue bothering world governments is the fact that Facebook plans to encrypt all these messages end-to-end. The United States government feels entitled access these communications based off the Communications Assistance for Law Enforcement Act (CALEA) which required ISP’s and telecom companies to allow law enforcement agents backdoor access to telecommunications data (Potasznik, Day 5). But Facebook isn’t classified as a telecom company, so it would seem that this bulk data collection wouldn’t apply to them. But even if
Facebook isn’t required to collect this bulk data, if the government has a warrant, Facebook is required by law to turn over those messages. Enforcement of a warrant can get tricky though, because if Facebook encrypts users’ messages end-to-end, the company can no longer see the contents of what users are sending each other. In other words, even if they were forced to, they wouldn’t be able to give the government any useful data.

The Department of Justice and its counterparts in the U.K. and Australia argue that end-to-end encryption would block their access to users’ communications and interfere with their ability to stop criminals and abusers (Dwyer, 2019). Those governments do have a point. There’s no disagreement that people use these messaging platforms to do very bad things. If the government can’t access what some suspected criminals are doing, it can lead to dangers in public safety and national security. So where is the line drawn? Should companies like Facebook give law enforcement access to their users’ data and messages?

Personally, I think law enforcement should have access to this data to better protect their citizens, but I am 100% sure if backdoors are created, they will be abused. Therefore, I am fine with companies encrypting their user’s data and not allowing law enforcement to access them. It’s a touchy subject without a clear answer as of now. Sooner or later, an incident will happen again like the San Bernardino case in which a government will ask a company to grant access to a suspected criminals’ messages or data and the company won’t be able to give access because they design their systems to be end-to-end encrypted.

References
