Thursday, March 24 2016

Dear Editor of the Observer,

My name is Tim Pusateri and I'm currently a senior computer science major here at Notre Dame. In recent months the issue of encryption has come to the political foreground and caused a significant degree of contention amongst politicians and business leaders alike. As a student who has studied encryption and its uses both inside the classroom and in a business setting, I feel there is a need for greater public understanding of encryption methods and how they affect our day-to-day lives.

Firstly, I feel the average technology user should be aware that virtually any information or communications they have on a device is encrypted. This means that when you enter a password or send an email, the actual data that gets transmitted across the internet or checked against a database is scrambled in a way that can be unscrambled. So much of the technological infrastructure that our society relies on is encrypted. This is a vital operation because computers are inherently open devices so that communication with other devices (an aspect that is central to modern computer operation) is possible and efficient. Encryption is what protects us from the scary scenarios in which an attacker intercepts our internet usage or gains unprivileged access to a server or database. However, there are varying degrees of encryption strength, and in the past, certain encryption methods how be broken and rendered defenseless to attackers. This is why computer security professionals are constantly doing everything they can to strengthen encryption and build safeguards against these types of attacks.

In light of the Apple vs. FBI debate, I feel everyone should understand these basics of encryption. We need to ask ourselves how much risk we are willing to take for the vast majority of lawful, everyday citizens to undermine the security of a minority of criminals. Of course if there was any easy way to break the security of criminals but not everyone else, we could do it. But the fact of the matter is there is not. This would be akin to building cars that can only go 30 mph for criminals, but lawful drivers have no limits on speed – it's just not realistic.

Students of Notre Dame, please take these thoughts into consideration. Before you speak on the matter of encryption and government ability to force Apple to weaken their security practices, take the time to educate yourself. This is a complex problem that computer scientists have been trying to solve since day one. Please do not think political rhetoric can solve in a news sound bite.

Thank you for your time,

Tim Pusateri