Alan Achkar, South Bend Tribune Editor
2323 South Bend Ave
South Bend, IN 46637

Dear Mr. Achkar,

I am writing to discuss the topic of encryption in today's technological world. As I'm sure you've noticed in the news, encryption has become quite the hot topic recently due to the case between Apple and the FBI about breaking encryption. Although I'm sure you are familiar, the story revolves around and iPhone recovered from a terrorism scene. The FBI speculates that the phone may have information leading to other attacks or possibly the terrorist cell itself. The phone is protected by a password. The FBI would like to use brute force to crack the password, but are not risking the possibility that the phone may have "delete after 10 attempts" turned on. This setting would cause the phone to dump all of its data if 10 failed password attempts were logged. The Bureau doesn't want the password – Apple doesn't even have this information – but instead, they would like Apple to create new firmware that would allow computerized brute force to unlock the phone. Apple refused, saying that that software could be incredibly harmful to customers if it ended up in the wrong hands. (Recent events point to a third party that says they could unlock the phone themselves, so the case has partially dissolved for the time being).

In case you're one of the less tech savvy editors around, I'll go through a quick encryption lesson to bring you up to speed. If you are already up to speed, feel free to skip over the rest of this paragraph! Currently, encryption is the safest way we know of to protect data. Encrypted data is entirely unreadable to the average eye/machine. It is known as cipher text, where unencrypted data is known as plain text. In order to make sense of encrypted data, a machine or user must have access to the key that decrypts it. In Apple's case, they were clear as to why they could not help the FBI from a data sense – the phone's data was encrypted, and per Apple's policy, the only machine with the key to decrypt data on the iPhone in question was that iPhone itself. Even if they wanted to, Apple couldn't decipher the data the FBI wanted. In an article in the Christian Science Monitor, Robert M Lee argues that "there is no way to grant access to encrypted data to the government without the method being abused," and I ask that you consider that statement yourself.

Without encryption, it is easy to see that data would be completely unsafe. Technology is never impermeable – even the strongest firewalls have tiny holes that can be climbed through. This leaves bank data, personal identification, medical records, and much more unprotected. But I don't believe that there is a debate over the existence of encryption. The question lies with who should be able to have the key. In the Apple case, the government argues that the data on the phone is a matter of national security and that they should be able to access it. But as Lee says, there's no way to ensure that the decipher methods will be used only as they are explicitly intended. Even if the permitted users were to stay exactly within their reaches, what would happen if another country's government were to get its hands on the

software? Who's to say they wouldn't use it to access some of the first government's data? Or even worse, what if a terrorist cell were to get access? Then the initial point is defeated and worsened by the tenfold. In a sentence, encryption breaking methods may never be abused, but there is no way to ensure that they will be secure. For this reason, I stand firm with the belief that encryption should remain a safe way to protect data from everyone, including government or other forces that may want access.

As you form your own opinion of encryption, I ask that you consider the subject on a more personal matter. The Apple case may be a matter of national security, but critical information of that sort is only a small fraction of encrypted data. As I mentioned before, all sorts of data is protected by encryption – bank data, social security numbers, medical records, etc. Consider your own bank data. If decryption methods ended up in the wrong hands, your bank data could end up in those hands as well. Imagine having $80k in your account on day and $0 the next. Or waking up one morning and realizing someone in the world has been impersonating you and living your life for years – opening credit cards in your name, spending your money, breaking down everything you worked hard to build up. Encryption does not only apply to government requested information; consider these facts before leaning one way or the other.

Thank you for your time in reading this letter. Please feel free to reach out if you have any questions or want to respond to any of the points I have made in this letter.

All the best,

HFred