ON JIM COMEY'S ATTEMPTS TO FORCE APPLE TO CHANGE ITS BUSINESS MODEL

As he has said repeatedly in Congressional testimony, FBI Director Jim Comey wants to change Apple's business model.

The former General Counsel for defense contractor Lockheed and hedge fund Bridgewater Associates has never, that I've seen, explained what he thought Apple's business model should be, or how much he wants to change it, or how the FBI Director put himself in charge of dictating what business models were good for America and what weren't and why we're even asking that in an age of multinational corporate structures.

It seems there are three possible business models Comey might have in mind for Apple:

- The AT&T (or Lockheed) model, in which a provider treats federal business as a significant (in Lockheed's case, the only meaningful) market, and therefore treats federal requests, even national security ones, as a primary market driver; in this case, the Feds are your customer
- The Google model, in which a provider sees the user's data as the product, rather than the user herself, and therefore builds all systems so as to capture and use the

maximal amount of data
- A different model, in which Apple can continue to sell what I call a walled garden to customers, still treating customers as the primary market, but with limits on how much of a walled garden it can offer

I raise these models, in part, because I got into a conversation on Twitter about what the value of encryption on handsets really is. The conversation suffered, I think, from presuming that iPhones and Android phones have the same business model, and therefore one could calculate the value of the encryption offered on an iPhone the same way one would calculate the value of encryption on an Android phone. They're not.

Even aside from the current difference between Google's business model (the data model at the software level, the licensing model at the handset level) versus Apple's model, in Apple's model, the customer is the customer, and she pays a premium for an idyllic walled garden that includes many features she may not use.

I learned this visiting recently with a blind friend of mine, whom I used to read for on research in college, who therefore introduced me to adaptive technologies circa 1990 (which were pretty cutting edge at the time). I asked her what adaptive technologies she currently uses, thinking that as happened with the 90s stuff the same technology might then be rolled out for a wider audience in a slightly different application. She said, the iPhone, the iPhone, and the iPhone. Not only are there a slew of apps available for iPhone that provide adaptive technologies. Not only does the iPhone offer the ability to access recorded versions of the news and the like. But all this comes standard in every iPhone (along with other adaptive

technologies that wouldn't be used by a blind person any more than most sighted ones). All iPhone users pay for those adaptive technologies as part of their walled garden, even though even fewer realize they're there than they realize their phone has great encryption. But because they pay more for their phone, they're effectively ensuring those who need adaptive technologies can have them, and on the market leader in handsets. Adaptive technologies, like online security, are part of the idyllic culture offered within Apple's walled garden.

The notion that you can assign a value to Apple's encryption, independent of the larger walled garden model, seems mistaken. Encryption is a part of having a walled garden, especially when the whole point of a walled garden is creating a space where it is safe *and easy* to live online.

Plus, it seems law enforcement in this country is absolutely obtuse that the walled garden does provide law enforcement access in the Cloud, and they ought to be thrilled that the best encryption product in the world entails making metadata — and for users using default settings, as even Syed Rizwan Farook seems to have been — content readily available to both PRISM and (Admiral Rogers made clear) USA Freedom Act. That is, Apple's walled garden does not preclude law enforcement from patrolling parts of the garden. On the contrary, it happens to ensure that American officials have the easiest ability to do so, within limits that otherwise ensure the security of the walled garden in ways our national security elite have been both unwilling and even less able to do.

But there's one more big problem with the fanciful notion you can build a business model that doesn't allow for encryption: Signal is free. The best app for encrypted calls and texts, Signal, is available free of charge, and via open source software (so it could be made available overseas if Jim Comey decided it, too, needed to adopt a different business model). The

attempt to measure in value what value encryption adds to a handset is limited, because someone can always add on top of it their own product, so any marginal value of encryption on a handset would have to make default encrypted device storage of additional marginal value over what is available for free (note, there is a clear distinction between encrypting data at rest and in motion, but the latter would be more important for anyone conducting nefarious actions with a phone).

Finally, there's one other huge problem with Comey's presumption that he should be able to dictate business models.

Even according to this year's threat assessment, the threat from hacking is still a greater threat to the country than terrorism. Apple's business model, *both* by collecting less unnecessary data on users and by aspiring to creating a safe walled garden, offers a far safer model to disincent attacks (indeed, by defaulting on encryption, Apple also made iPhone theft and identity via device theft far harder). Comey is, effectively, trying to squelch one of the market efforts doing the most to make end users more resilient to hackers.

The only model left—that could offer a safer default environment—would effectively be an AT&T model pushed to its limits: government ownership of telecoms, what much of the world had before Reagan pushed privatization (and in doing so, presumably made the rest of the world a lot easier for America to spy on). Not only would that devastate one of the brightest spots in America's economy, but it would represents a pretty alarming move toward explicit total control (from what it tacit control now).

Is that what former Hedgie Jim Comey is really looking to do?

One final point. While I think it is hard to measure marginal value of encryption, the recent kerfuffle over Kindle makes clear that the market does assign value to it. Amazon dropped

support for encryption on some of its devices last fall, which became clear as people were no longer able to upgrade. When they complained in response, it became clear they were using Kindles beyond what use Amazon envisioned for them. But by taking away encryption users had already had, Amazon not only made existing devices less usable, but raised real questions about the CIA contractor's intent. Pretty quickly after the move got widespread attention, Amazon reversed course.

Even with a company as untrustworthy and data hungry as Amazon, removing encryption will elicit immediate distrust. Which apparently is not sustainable from a business perspective.