CRYPTOME

Refuting David Cameron's Privacy Talking Points

Lies My Teacher Told Me about Cryptography

By **Bill Blunden**, January 17, 2015

In the wake of the Charlie Hebdo shootings prominent officials in the UK like MI5 chief Andrew Parker and Prime Minister David Cameron have appealed for greater authority with regard to mass surveillance. These requests are drawn from the same playbook that was employed in the United States after 9/11. The political operatives of the 1 percent never let a disaster go to waste.

Leveraging public anxiety surrounding terrorist plots and ongoing police raids Parker warned an audience at MI5 headquarters that an impending attack was "highly likely" and that in order to safeguard the public civil liberties would have to take a back seat to national security. Parker stated:

> "I don't want a situation where that privacy is so absolute and sacrosanct that terrorists and others who mean us harm can confidently operate from behind those walls without fear of detection."

Likewise David Cameron stressed that there should be no "means of communication" which "we cannot read" in an effort to eliminate "safe spaces for terrorists to communicate."

On an aside, the whole argument that society must yield privacy on behalf of security is essentially a form of extortion based on a false dichotomy. Officials claim that unless we hand over our civil liberties they can't protect us from whatever awful things await. Despite the fact that history has proven mass surveillance as a fairly inert tool for thwarting terror. Instead, the essence of surveillance is control, and the more privacy that we yield the more control society hands over to the small group of people wielding the global panopticon. Benjamin Franklin's pithy observation still holds:

> "They who can give up essential liberty to obtain a little temporary safety, deserve neither liberty nor safety."

Anyway, the *Guardian* indicates that Prime Minister Cameron has spoken with Obama in an effort to persuade companies like Google and Apple, which have deployed encryption technology, to cooperate with British intelligence so that government spies get the data they need to "keep us safe." More specifically, Cameron wants to work with companies to "devise ways to obtain more access to encrypted messages on the Internet between terrorists."

This sounds a lot like a bid for what's known as "key escrow." The basic idea is that online service providers configure their products with special decryption passwords (also known as a decryption *keys*) which are then held in escrow. With the necessary legal justification, like a court order, law enforcement

can acquire decryption keys from a service provider and monitor network traffic in its unencrypted state.

On the surface Cameron is making an unabashed big brother move by prodding corporate America for something like key escrow. On a deeper level Cameron's diatribe against encryption can, like that of FBI Director James Comey, be viewed as a subtle form of advertising. The tacit message is that encryption is such a formidable defense that security services are completely powerless against it (gasp!).

This message ignores a reality made clear by leaked classified documents: that encryption is all good and well… that is, until protocols are weakened, implementations are subverted, or encryption keys are acquired (by hook or by crook).

Such countermeasures are brandished on a much larger scale than most people presume and without the drama of David Cameron's public gripes. Think of it this way, if government spies can get a security company like RSA to add some special sauce to their products the end result can spell back door access into thousands of allegedly high-security environments. Once more there are classified programs that span the entire American hi-tech industry.

It's part of the public record that GCHQ has refined a "capability against Cisco routers." Given Cisco's market share the implications are unsettling. The prospect of hardware subversion was enough to push Russian intelligence, which boasts some of the best players on the field, to revert to typewriters.

Hence Internet users are admonished to be wary of security promises as they tend to conceal security landmines. Don't *ever* take guarantees of anonymity at face value (especially if they arise from the U.S. State Department). Expect betrayal and plan accordingly. This isn't privacy nihilism on behalf of your humble narrator but rather justifiable caution. Be careful of the tools you use and how much trust you put in them. And, whatever you do, don't rely on security vendors to magically endow you with genuine security. They're too busy chatting up spy masters on a first-name basis.

Bill Blunden is an independent investigator whose current areas of inquiry include information security, anti-forensics, and institutional analysis. He is the author of several books, including *The Rootkit Arsenal* and *Behold a Pale Farce: Cyberwar, Threat Inflation, and the Malware-Industrial Complex*. Bill is the lead investigator at Below Gotham Labs.