Stoked by Bond and other fiction, our fear of surveillance is worse than the real thing

November 4 2015, by Brandon Valeriano

Credit: cottonbro studio from Pexels

The latest Bond film, *Spectre*, presents 007 with the very modern problem of cyber-security. Yet Bond cares more about being right, and about revenge – against both the man who wronged him and the government's efforts to put the "00" spy programme out of business by replacing it with better information – the sort of broad data collection and sharing that gets a bad rap. Bond is a fictional character, but his reaction follows the public's inability to understand how this sort of information sharing is necessary.

In the film, the shadowy Nine Eyes initiative collects and stores intelligence information from the nine most active espionage states, giving it the ability to predict and intervene before events happen. In reality, this is an invented fiction – one created by filmmakers and writers, but also by our own minds.

The recent coverage of the Cybersecurity Information Sharing Act (CISA) passed by the US senate only reinforces the view that the fears we construct are often the greatest danger to our security. An all-knowing security surveillance programme is beyond our capabilities at the moment, but by preventing government and commercial organisations from making best use of the information available to them, we're leaving ourselves vulnerable.

In truth, the idea of James Bond-style characters is entirely antiquated. A brute force instrument trained to kill despite the costs – the opening scene of the film sees him apparently killing hundreds on the justification of saving thousands. Bond has become a drone, capable of being sent in to terminate suspects, and quite probably causing high levels of collateral damage in the process. Better information on security threats would help us to minimise the need for such brute force.

Critics and limitation

In Spectre, the dangers posed by Nine Eyes are all too realistic for modern audiences. The problem with bulk data collection programmes is not the invasion of privacy but the possibility these programmes would be used for negative ends. While the film poses this as real – given the limitations within CISA – this is still fantasy. In fact CISA, which is designed to encourage businesses and government agencies to share information related to malicious hackers and their methods, is so limited in scope it's in danger of being ineffective.

Bulk data collection is voluntary, possible only when targets cooperate with the US government after a cyber-attack. Our fears of data collection and information gathering are often overblown. Take for example how the Guardian newspaper refers to the programme, calling it "the bill critics say will allow the government to collect sensitive personal data unchecked." US citizens already face bulk data collection, carried out by the National Security Agency and in violation of US law. And businesses already face bulk data collection of a different kind, as demonstrated by the hack and theft of millions of TalkTalk customers.

CISA is not perfect. Removing the right for citizens to make Freedom of Information requests for their own personal data is a strange incentive included in the bill. It's true that many industries already have methods to share information on cyber-threats, but without any standardisation. Hopefully the bill would help figure out how to improve this situation. Bulk data would only be shared in the context of an ongoing threat or violation. In other words, when at the point that the (for example) TalkTalk hacker has already stolen your personal data, why would you be concerned that the same information would be shared with government agencies?

There is a real need to rectify our fears and align them with the realities of cyber-conflict. Yes, we face a growing number of attacks online, but their impact and severity are not increasing. To secure this fragile stability, we need to take an approach that will ensure that those attacks and breaches that are bound to occur are kept as limited as possible.

Incident reporting, working with the government, and providing information on all the technical details of cyber-attacks is a critical step needed to ensure we're protected against this 21st-century threat. In fact, I'd say we need more than voluntary information sharing; we need mandatory sharing of information and cooperation when these attacks happen.

As tends to happen, corporations run to government when they need protection, but they should also bear the responsibility to be prepared to help the government out as well. Bulk data collection systems can be dangerous, but as long as they are run by responsible government agencies – and not branches of shadowy criminal organisations like Spectre – we can hope to turn them into an effective bulwark against cyber-attacks.

These are the sorts of systems that should replace the Bonds of the world. If were are going to share inmate secrets online, we must also understand that this makes us vulnerable and protections are needed. The US needs CISA, and more, just as the UK needs something similar – despite the fears this data will be in the hands of some criminal mastermind in a Nehru jacket with a white cat.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation

Citation: Stoked by Bond and other fiction, our fear of surveillance is worse than the real thing (2015, November 4) retrieved 16 August 2024 from https://phys.org/news/2015-11-stoked-bond-fiction-surveillance-worse.html