The FBI Uses "Abhorrent Crimes" to Extend its Digital Reach

When it comes to the web, the long arm of the law is going global.

Graham Templeton

March 28, 2017

or more than three years, Eric Eoin Marques has been sitting in a jail cell in Ireland, fighting the global legal system for the right to plead guilty to truly horrible crimes. Last month he finally lost, and as a result, Marques will soon be extradited to America to face a maximum 100-year sentence. In Ireland, he would face a maximum sentence of just *eight* years.

His case poses a far-reaching question about the trajectory of global law enforcement with respect to cyber crime, and the nature of crime and justice in a connected world. The uncertainty of the legal space is allowing law enforcement agencies like the FBI to acquire wide-ranging powers of which they quite recently could not have dreamed.

"The U.S. government is exploiting the fact that a lot of these cases are about the most abhorrent crimes, like child pornography," UC Hastings law professor Ahmed Ghappour tells *Inverse*. Indeed, the FBI has accused Marques of running a network of encrypted servers, the content of which made him the "largest facilitator of child porn" on the internet — but it's unclear just which aspects of his crime entitle the United States to try the case.

"[This sort of case] allows law enforcement to set up structures that wind up depriving all of us of rights, not just the bad guys," Ghappour says.

With respect to Marques, the right in question was the right to know *which* laws applied to his crime. His actions were taken in Ireland, via servers reportedly located all over Europe, and yet he was arrested "for the purpose of his extradition" to be tried before the American system of law. For so-called *crimes of a cyber nature*, legal jurisdiction can be precisely what any two international governments would like it to be.

To understand the generality of the arguments at work here, it's necessary to quickly review the facts of the case: Marques ran an encrypted hosting service called Freedom Hosting, and its main selling point was that it had been set up so that nobody — including Marques himself — could know a customer's identity or the content of their hosted space. This might have made for an intriguing argument about technologically maintained plausible deniability, but police quickly referenced the existence of chat logs proving Marques was "well aware" of how his servers were

being used. Seeing that Marques had little to no chance of acquittal, the defense decided that it had to settle for a guilty plea — but no charges ever came. Though he was denied bail as a flight risk, Marques was held by the Irish only in lieu of being shipped out to the United States.

It should be pointed out that the FBI invested virtually all of the money and manpower needed to conduct this technologically unprecedented investigation into encrypted dark web hosting, and to eventually bring Marques to justice. The Bureau declined to comment for this piece, but the agency's motivations for requesting the extradition are likely diverse, from the wish to have Marques on hand to assist further prosecutions to the simple desire to see bad guys get appropriately harsh punishments. With Marques in Ireland and the servers all over Europe, however, the question was how the FBI would argue that the United States had been involved, at all.

Testifying at the initial extradition hearing, the FBI agent in charge revealed some details of the investigation and laid out a compelling case that Marques should be tried *somewhere* for the crime — but on the topic of America's specific need to try the case, most of the discussion seems to have been about the differences between the American and the Irish sentencing guidelines. To allow Marques to be extradited to face American law, Ireland's Director of Public Prosecutions (DPP) has been forced to claim the office's "long-standing" immunity from "having to explain its decisions."

If Marques was looking to invoke some sort of right to plead guilty to a crime within his native country, the Irish appeals judge made the situation clear: "There is simply no such right known to the law."

The defense tried a variety of tactics to delay the extradition and bring attention to the case. From arguing that Marques couldn't be extradited because he has Asperger syndrome, to attacking the integrity of the U.S. justice system and the supposed likelihood that the FBI would torture Marques, they threw a lot at the judge.

None of it worked and, unsurprisingly, the case of this enigmatic dark webmaster described as a loner who struggled to complete his schooling, has attracted very little attention.

There was one objection raised by an Irish human rights group that challenged the DPP — the country's public prosecutor — for refusing to give reasons *for not giving reasons* for its decision not to prosecute Marques in Ireland. So, the DPP could claim it doesn't want to give its reason for allowing the extradition, then explain *that* decision as having to do with, for instance, not tipping off suspects in other, ongoing investigations. The DPP has refused to provide even that sort of meta-explanation.

If Irish authorities had explained why they chose not prosecute Marques, it would have at least produced some valuable insight into the *types* of arguments that are considered valid with respect to crimes committed online.

It could also have forced the DPP to admit if its decision was made specifically to expose Marques to a harsher American sentence than the Irish system allowed, or because in many countries the FBI quite simply gets whatever it asks for.

Ghappour says that the long arm of American law began to truly reach into foreign countries with the passing of the Patriot Act.

"In addition to the multitude of civil liberties that it deprived Americans," he explained, "[the Patriot Act] also basically wholesale took a bunch of laws and made them extraterritorial. So now in the United States, we have a lot of statutes that have extraterritorial application … even if all the conduct happens abroad."

All the United States has to do to make a request is prove that is has been at least peripherally affected by the crime — and as the Marques extradition shows, that effect can be as peripheral as having citizens who *theoretically* have been exposed to an illegally hosted file. Like every other bit of data on the regular internet and dark web alike, the services on Freedom Hosting were available all over the world. Thus the entire connected world, from the United States to Russia, could make a claim to have been harmed by it.

Regardless of the country, it's simply hard to pass new laws, and this results in a global preference to simply apply existing policies in new contexts that their drafters never could have imagined. Temple University professor and Cato Institute scholar David G. Post tells *Inverse* that when it comes to online crime, "it's just like he's standing on the border and sending things — papers, dirty books — over the border into the United States."

To figure out just how far this expansion of global cyber jurisdiction could reach, *Inverse* asked international legal expert Dapo Akande, one of the drafters of the newly released Tallinn Manual 2.0, the authoritative modern guide to global cyber law. The Tallinn approach is not to propose new cyber laws, but to do precisely what Post described: interpret existing laws for the cyber age.

For example, if someone in Chicago leaves a YouTube comment that's considered hate speech in some countries — but which is legal in the United States — Akande says the law offers little to no protection. "It can still be viewed in France, in Austria, in Germany, where it might be criminal. You could actually be subject to the jurisdiction of practically every single country in the world, on the basis that you've committed a crime within their territory."

Traditionally, there have been two principles protecting citizens from law enforcement in other countries: One was that a crime had to affect another country, and the other was that if the accused's own country agreed that a crime had been committed, it would almost always want to try the offender itself. The Marques case shows that a claim of specific national harm can be a simple gimme in cyber cases, and protection by one's home country is a privilege that not everyone enjoys.

In the example of a hateful YouTube comment, the offender is likely safe. America and its law enforcement agencies do more *making* of demands than taking them. If you're a citizen of a less dominant country, on the other hand, the shifting loyalties of international politics will determine your fate. Right now, the state of global politics is such that Ireland is friendly to the FBI's request for Marques, and thanks to the generality of cyber law, that friendliness is sufficient to allow the extradition.

So, can any cyber crime be prosecuted in any jurisdiction in the world? "Kind of, yes," Post says.

Though he admits it was less likely to become an issue, Post points out that these laws are supposed to be basically symmetrical. "The United States has to be prepared for the notion that Ireland might assert jurisdiction over someone here," he says.

Played out long enough, these sorts of trends could be used not just to apply U.S. laws to non-U.S. citizens, but to send U.S. citizens to face non-U.S. laws. That sort of power could allow nations to be set up as a dumping grounds where suspects receive reliably harsher or easier sentences. Or cases just might disappear entirely. Similar schemes have been tried in the past.

As a point of comparison, just two years before Marques' arrest, Ireland refused a request for the extradition of Sean Garland, accused of making and circulating large quantities of counterfeit American currency. Garland was kept in Ireland on the grounds that while these offenses affected the U.S. and U.S. interests, they were still committed on Irish soil. The international movement of these counterfeit physical objects did not confound the law as thoroughly as the international movement of data.

The Department of Justice declined to comment on our requests for clarification on the legal issues surrounding cyber jurisdiction, referring instead to the existingdomestic U.S. statutes on child exploitation, and the similar extradition of Kenyan national Brian Musomba Maweu. Maweu was also extradited to the United States for posting child porn images entirely from abroad — but the principle of jurisdiction was less relevant in that case because Maweu chose to waive his right to object to the extradition.

As more criminals take their trade online, and more online actions potentially become criminal, more people will be subject to this poorly defined area of meta-law, in which any number of equivalent legal situations all simultaneously threaten to apply from different nations around the world.

The breadth of these legal principles extends beyond the horrible crimes that are setting much of the precedent. It's worth remembering that in the days after the arrest of Marques, the FBI operated the Freedom Hosting servers as part of a sting operation, and attempted to transmit spying malware to every single user who connected to them, for any reason.

That might not seem such a bad thing to do to child pornographers, but in addition to the heinous criminal content, Freedom Hosting's security also attracted legitimate customers like TorMail, which was by far the largest encrypted email service at the time of its takedown. It was used widely by journalists, activists, and dissidents all over, but both the power and ambiguity of the investigation allowed law enforcement to compromise their security, right alongside criminal users.

In cases like this, the FBI's first and foremost goal is pursuit of justice — certainly, most people would likely agree that Marques' crimes warrant closer to the American sentencing guidelines (throw away the key), than the Irish sentence (less than a decade).

This is why the Marques case is so important for other cases. Seemingly simple logic, in the context of the unprecedented scope of cyber law, can turn good single acts into cascades of worrying consequences.

Troubling as the Irish sentencing guidelines may be, its laws will never change if an international shell game swaps in foreign laws to replace them at will.

Akande says an international treaty for mutually agreed-upon rules of cyber jurisdiction is unlikely. “This will be resolved in the way of all international law,” he said. “It will be figured out through state action.”

In other words, it will likely take at least a few high-profile examples of overreach to generate enough public outcry to slowly recalibrate the system toward reasonable jurisprudence. All any one person can do until then is hope not to become one of those cautionary case studies along the way, subjected to a legal tradition that was designed for offenders like Marques but which was always going to be applied as widely as possible.