CASE STUDY

Greg Maroon was emboldened.

Flanked by his attorneys, Maroon strode confidently out of the grand jury room on the 15th floor of the Phillip Burton Federal Building in San Francisco. Each day for the past three months, Maroon had lived with the possibility that he would be ordered to federal prison for his refusal to comply with a federal grand jury subpoena. Finally, he thought to himself, it was over.

Maroon told his attorneys to go ahead, and that he would catch up with them. He sat down beneath one of the large, black-and-white photographs that lined the hallway, gifts donated by The Hon. Alex Weld, a former reporter and the same federal magistrate who had just ensured Maroon’s continuing freedom.

Maroon’s scanned Judge Weld’s order granting in part and denying in part his motion to quash the federal subpoena. The subpoena had commanded Maroon to turn over an encrypted file that had been found on his computer, “Central Java interviews with J-I, 2013-10-24,” in its unencrypted form or, in the alternative, to provide the grand jury with his password. The order held that Maroon had to turn over his copy of the encrypted file, as its existence was a foregone conclusion. Maroon wasn’t too worried about this, however, as the government had possessed a copy of the encrypted file for months; turning it over would add nothing to the information in the government’s possession.

Maroon read on. The court analyzed the decryption issues carefully, concluding that decrypting the file or providing the password was testimonial in nature, and that it therefore triggered the Fifth Amendment privilege against self-incrimination. The court also held that the foregone conclusion doctrine did not apply to the act of decryption or production of the password, as the government had not made a sufficient showing regarding the contents of the Central Java file. (Although not in the public Order, after being presented with classified evidence of Maroon’s connections with terrorism suspects in camera, Judge Weld noted to the federal prosecutor that the calls were all domestic; since a federal judge ruled in December 2013 that the NSA’s domestic call tracking program violates the Fourth Amendment, Judge Weld noted, the calls might also be unusable even if relevant. At that point the prosecutor conceded that DOJ probably would not appeal the ruling on the self-incrimination issue.)

Satisfied with the result of the hearing, Maroon got up and joined his attorneys to celebrate.

A month later, Maroon was standing in a convention center in Reno, speaking with a friendly, slightly nerdy fellow named Marc. Maroon and Marc were both in town to attend the annual ‘RAD

CON’ conference, which includes a motley crew of black hat hackers, security researchers, surveillance company representatives, journalists and — though they were ‘uninvited’ for the first time ever due to revelations about government surveillance — undercover federal agents seeking to learn about new techniques, tools and trends.

Marc had commented on the EFF sticker on Maroon laptop while the two were standing in line for coffee, and they immediately hit it off. Upon learning that Maroon was from Seattle, Marc shared that he too was from the Pacific Northwest, confiding that when he was in college he would take a Zipcar from Portland to Seattle on an almost weekly basis to engage in acts of petty vandalism against corporate property. He said he mostly broke windows at Starbucks stores, mostly just by default. Maroon volunteered that he did the same kind of thing in Oakland in 2011.

Over the next few days, the two men grew close. They fretted over NSA surveillance, brainstormed about how to weaponize the Freedom of Information Act, damned The Man, and extolled the virtues of black hoodies. At the end of the conference Maroon and Marc exchanged vCards via Bluetooth. They promised to keep in touch.

There was just one problem: ‘Marc’ wasn’t real, but a cover identity. The name ‘Marc’ itself was a self-referential portmanteau of “masterful narc.” Maroon had just become BFFs with Special Agent Andy Security.

And who could blame him? SA Security spent months reviewing publicly-available information, including information Maroon posted to social networking websites, and tailored his carefully-crafted character to befriend Maroon, earn his trust and exploit the relationship to gain relevant information about Jemaah Islamiyah.

To that end, prior to tailing Maroon to Reno, SA Security prepared a special vCard file loaded with a customizable surveillance FBI payload, the same vCard he transmitted to Maroon’s phone. As configured, the script inside the vCard was set to note calls to or from individuals on the terrorist watch list, and then only the numbers dialed. The program would then transmit this information securely to an FBI server, where SA Security could review it.

Unaware of all this, and newly-inspired by what he thought was his super cool new hacker friend’s willingness to fight The Establishment, Maroon decided to find out more about the phone call he had received from SA Security. He drafted a dozen detailed FOIA requests and sent them off to them FBI. Maroon then got back to work on a story about extremism for Frontpage, a PBS program, which included portions of his interviews with members of Jemaah Islamiyah in Indonesia.

When Maroon called his sources to fact-check the story, SA Security’s email went haywire. SA Security began receiving dozens of alerts generated by the vCard payload showing that Maroon’s phone was connecting to the phones of numerous radicals in Indonesia, including individuals thought to be directly responsible for several terrorist attacks, people the U.S. government had been trying hard to track down. Based on this information, SA Security immediately prepared a search warrant for Maroon’s published and unpublished journalistic materials, as well as a subpoena for his Gmail account, the contents of which were produced.

At 5:29 a.m. the next morning, an FBI SWAT team armed with assault rifles broke down the door to Maroon’s North Berkeley apartment, detonated flashbang grenades and detained Maroon at gunpoint. But the concussions of the flashbangs going off were no match for the shock Maroon felt when ‘Marc’ walked in wearing an FBI raid jacket and wordlessly handed Maroon a copy of the search warrant. To make matters worse, ‘Marc’ seemed to be in charge: at direction the raid team seized notes, computers, iPads, CDs, unpublished photographs, and a huge number of documents that appeared to be from the FBI itself.

Maroon was not arrested, and the raid team did not find a USB drive he had hidden in his sock as they came storming down the hall toward his bedroom. As soon as he was sure the agents were gone, Maroon rushed to his local library and typed up a news story detailing everything he could piece together about the events that had transpired since he got off the plane at SFO. This included information about SA Security’s disciplinary records, which the FBI had inadvertently released. The records showed that SA Security was about to lose his job for subpoenaing Maroon without first seeking U.S. Attorney General approval — or anybody else’s approval, for that matter. Maroon published the story on Indybay, a local online-online news outlet.

A couple of weeks later, SA Security was indeed fired, in part for events related to the subpoena of Maroon, and in part for the later events. Former SA Security then filed a lawsuit against Maroon and the FBI in federal court pursuant to FOIA and the Privacy Act. He also included a state law claim for public disclosure of private facts, which is allowed under what is known as “pendent jurisdiction”.