CHAPTER IV

# Legal Cases Around the World

(with Jelena Ardalic)

Extensive case-law review revealed a paucity of reported cases on ethical hacking worldwide. Cases that were reported are published in legal databases. We looked at legal databases for all Commonwealth countries (United Kingdom, Australia, Canada, etc.) as well as the United States, Israel, Indonesia, Japan, Singapore, and Germany. The lack of cases is likely due to three key factors:

1. the currency of the actions (insufficient time for a trial or a decision to have been reported in case-law databases),
2. the accused may have settled the case, or
3. the accused may have agreed to act as an informant in exchange for dropped charges.

The other important factor, as will be explored in chapter 12, is that there are many technical and legal challenges that make investigation and prosecution difficult. Hacking often includes obfuscation technologies routed through multiple jurisdictions. Attribution is the greatest challenge for cybercrime—while you may be lucky enough to trace a communication to a device, device location tracking is often only accurate to a four-block radius, and even if you can drill down to a device, you must prove who the person was who used the device.

This chapter catalogues case law globally, based on jurisdiction, starting with the United States, which has the greatest number of

reported cases. We itemize the cases, provide facts, then categorize the case by country, case name, citation, jurisdiction, main URL, charge, legislative provisions, main target, motivation, conviction, sentence, and additional important information.

## UNITED STATES

### *United States of America v. Bradley Manning*

The defendant was arrested after allegedly accessing and providing classified US government documents to WikiLeaks. Private First Class Manning was a US Army intelligence analyst based in Iraq and was charged in 2010.

| ITEM | NOTES |
|---|---|
| Case name: | *United States of America v. Bradley Manning* |
| Citation: | *E., PFC* (2013) |
| Jurisdiction: | United States Army Military District of Washington |
| Main URL: | Wikipedia, *United States v. Bradley Manning* (July 25 2018) http://en.wikipedia.org/wiki/United_States_v._Bradley_Manning.<br><br>United States Division—Center, "Soldier Faces Criminal Charges" (media release, no. 20100706-01, July 6, 2010).<br><br>Associated Press, "Panel Says WikiLeaks Suspect is Competent to Stand Trial," *New York Times*, April 29, 2011, available at http://www.nytimes.com/2011/04/30/us/30brfs-PANELSAYSWIK_BRF.html?_r=1&ref=bradleyemanning. |
| Charged with: | Transferring US government documents to a party not entitled to receive them (Julian Assange of WikiLeaks) |
| Legislative provisions: | Uniform Code of Military Justice articles 104 (aiding the enemy), 92 (failure to obey a lawful order or regulation), 132 (general article, including counts of offenses against the Computer Fraud and Abuse Act 1986 (18 *United States Code* [hereinafter, U.S.C.] section 1030(a)), and 793 (communicating, transmitting and delivering national defence information to an unauthorized source) |
| Main target: | US Army and US government |
| Motivation: | Public disclosure of US government (including foreign policy) documents in order to "change something" (according to the transcript of his chats with hacker Adrian Lamo, see Wikileaks, for example at https://www.youtube.com/watch?v=lzwUeqC8E60) |

| | |
|---|---|
| Convicted of: | Convicted of committing nineteen of the twenty-two charges, but acquitted of aiding the enemy by knowingly providing the enemy with intelligence through indirect means |
| Sentence: | On August 21, 2013, Manning was sentenced to thirty-five years in prison. On January 17, 2017, then-US President Barack Obama commuted Manning's sentence to a total of seven years' confinement, starting with the initial date of arrest. As a result, Bradley Manning, now known as Chelsea Manning, was released on May 17, 2017 |
| Additional important information: | Twenty-two charges under the Espionage Act, including aiding the enemy and improperly obtaining a classified gunsight video. Proceedings commenced in Forte Mead, Maryland, February 23, 2011.<br><br>Manning was nominated for a Nobel Peace Prize on February 27, 2011. The increased media attention reflects contemporary attitudes toward hacktivism. |

### *United States of America v. Kevin George Poe*

An Anonymous-affiliated Connecticut man, Poe (handle: "spydr101"), was arrested and charged with conspiracy and unauthorized impairment of a protected computer after allegedly disabling rock musician Gene Simmons's website with a denial-of-service attack.

| ITEM | NOTES |
|---|---|
| Case name: | *United States of America v. Kevin George Poe* |
| Citation: | CR 11 01166 |
| Jurisdiction: | United States District Court for the Central District of California |
| Main URL: | J. Zand, "Indictment Alleges DDoS Attack on Gene Simmons' Web Site by Anonymous Supporter" on *Justia Law Blog* (December 14, 2011), available at http://techlaw.justia.com/2011/12/14/indictment-alleges-ddos-attack-on-gene-simmons-web-site/.<br><br>J. Halliday, "Gene Simmons gets kiss of death from notorious web forum," *Guardian*, October 14, 2010, available at http://www.guardian.co.uk/technology/blog/2010/oct/14/gene-simmons-anonymous-attack-filesharing. |

| | |
|---|---|
| | The Smoking Gun, "Plea Deal Struck Over Attack on Kiss Web Sites," February 5, 2013, available at http://www.thesmokinggun.com/documents/gene-simmons-ddos-plea-587912.<br><br>G. Aegerter, "13 Alleged Members of Anonymous Hacking Group indicted, accused of Participating in Operation Payback," *NBC News*, November 3, 2015, available at https://www.nbcnews.com/news/world/13-alleged-members-anonymous-hacking-group-indicted-accused-participating-operation-flna8C11332039. |
| Charged with: | Conspiracy and unauthorized impairment of a protected computer |
| Legislative provisions: | 18 U.S.C. sections 371 (conspiracy), 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(I) (unauthorized impairment of a protected computer) |
| Main target: | Gene Simmons via his website |
| Motivation: | Likely to be protest or retribution as the crime occurred shortly after Gene Simmons criticized file sharing and encouraged copyright owners to commence litigation and seek extensive damages against file sharers (see the cited *Guardian* article for screenshot of Anonymous message about Gene Simmons's views) |
| Convicted of: | Poe pleaded guilty. As part of a plea agreement, he was charged with the reduced impairment count. |
| Sentence: | Initially, if convicted of both counts, Poe would have faced up to fifteen years in federal prison. However, after pleading guilty to the reduced impairment count and reaching a plea agreement, he was sentenced to home detention and probation |
| Additional important information: | Used Low Orbit Ion Cannon software to instigate attack |

### *Member of LulzSec Arrested for June 2011 Intrusion of Sony Pictures Computer Systems*

"A member of the LulzSec hacking group was arrested…for his role in an extensive computer attack against the computer systems of Sony Pictures Entertainment.… On September 2, 2011, a federal grand jury returned an indictment filed under seal in US District Court in Los Angeles charging [Cody] Kretsinger with conspiracy and the unauthorized impairment of a protected computer" (FBI).

| ITEM | NOTES |
|---|---|
| Case name: | *United States of America v. Kretsinger* |
| Citation: | 2:11-cr-00848 |
| Jurisdiction: | United States District Court, Central District of California (Los Angeles) |
| Main URL: | FBI, "Member of Hacking Group LulzSec Arrested for June 2011 Intrusion of Sony Pictures Computer Systems" (press release, September 22, 2011), available at http://www.fbi.gov/losangeles/press-releases/2011/member-of-hacking-group-lulzsec-arrested-for-june-2011-intrusion-of-sony-pictures-computer-systems (last accessed October 20, 2011).<br><br>C. Arthur, "Alleged LulzSec hacker of Sony Pictures faces trial data in December," *Guardian*, October 18, 2011, available at http://www.guardian.co.uk/technology/2011/oct/18/lulzsec-alleged-recursion-hacker-trial.<br><br>D. Whitcomb, "Hacker Gets a Year in Prison for Sony Attack," *Sydney Morning Herald*, April 19, 2013, available at https://www.smh.com.au/technology/hacker-gets-a-year-in-prison-for-sony-attack-20130419-2i4hl.html. |
| Charged with: | Conspiracy and the unauthorized impairment of a protected computer (using an SQL injection and a proxy server) |
| Legislative provisions: | Most likely to be 18 U.S.C. section 1030(a)(2) |
| Main target: | Sony Pictures Entertainment's computer systems |
| Motivation: | Follow-up attack to Sony PlayStation network hack. Proof of ability to exploit global conglomerate with ease: "'From a single injection we accessed EVERYTHING,' the hacking group said in a statement at the time. 'Why do you put such faith in a company that allows itself to become open to these simple attacks'" (Arthur). |
| Convicted of: | Unauthorized impairment of protected computers |
| Sentence: | On April 19, 2013, Kretsinger was sentenced to one year in federal prison, along with one year of home detention after the completion of his prison sentence, $605,663 in restitution to Sony Pictures, and 1,000 hours of community service |
| Additional important information: | Used an "SQL Injection attack" as means of gaining access and gathering information (per Arthur).<br><br>Kretsinger's handle: "recursion." |

***United States of America v. Daniel Spitler and Andrew Auernheimer***

"Two self-described Internet 'trolls' were arrested…for allegedly hacking AT&T's servers and stealing e-mail addresses and other personal information belonging to approximately 120,000 Apple iPad users who accessed the Internet via AT&T's 3G network" (FBI). The defendants are alleged to be associates of the group Goatse Security, which, according to Wikipedia, is a grey-hat hacker group that exposes security flaws. (So, in this sense, vaguely "ethical.")

| ITEM | NOTES |
|---|---|
| Case name: | *United States of America v. Daniel Spitler and Andrew Alan Escher Auernheimer*; Appeal: *Auernheimer v. United States of America* |
| Citation: | Mag. No. 11-4022 (CCC); Appeal: Third US Circuit Court of Appeals, No. 13-1816 |
| Jurisdiction: | Newark, New Jersey |
| Main URL: | FBI, "Two Men Charged in New Jersey with Hacking AT&T's Servers" (press release, January 18, 2011), http://www.fbi.gov/newark/press-releases/2011/nk011811.htm.<br><br>Criminal Complaint: http://www.justice.gov/usao/nj/Press/files/pdffiles/2011/Spitler,%20Daniel%20et%20al.%20Complaint.pdf.<br><br>E. Mills, "AT&T-iPad hacker pleads guilty to computer charges," *Cnet*, June 23, 2011, available at http://news.cnet.com/8301-27080_3-20073791-245/at-t-ipad-hacker-pleads-guilty-to-computer-charges/.<br><br>E. Mills, "AT&T-iPad site hacker to fight on in court (exclusive)," *Cnet*, September 12, 2011, available at http://news.cnet.com/8301-27080_3-20105097-245/at-t-ipad-site-hacker-to-fight-on-in-court-exclusive/.<br><br>T. McCarthy, "Andrew Auernheimer's conviction over computer fraud thrown out," *Guardian*, April 12, 2014, available at https://www.theguardian.com/technology/2014/apr/11/andrew-auernheimers-weev-conviction-vacated-hacking. |
| Charged with: | "Each defendant is charged with one count of conspiracy to access a computer without authorization and…fraud in connection with personal information" (per the FBI) |
| Legislative provisions: | 18 U.S.C. sections 1030(a)(2)(C), I030(c)(2)(B)(ii), and 371 |
| Main target: | AT&T's servers, specifically those handling 3G iPad traffic |

| | |
|---|---|
| Motivation: | Possibly to publicize security faults in AT&T's 3G network, or for "criminal gain or prestige among peers in the cyber-hacking world" (per the FBI) |
| Convicted of: | Conspiracy to gain unauthorized access to AT&T public servers |
| Sentence: | "Each count with which the defendants are charged carries a maximum potential penalty of five years in prison and a fine of $250,000" (per the FBI).<br><br>Spitler pleaded guilty in June 2011 and was sentenced to three years' probation. Spitler was also ordered to pay $73,167 in restitution.<br><br>In 2014, the US Court of Appeals for the Third Circuit Court threw out the convictions against Auernheimer on the basis that the prosecution did not belong in New Jersey. As a result, his November 2012 conviction and forty-one-month prison sentence could not stand. |
| Additional important information: | Andrew Alan Escher Auernheimer's handle: "weev."<br>Daniel Spitler's handle: "JacksonBrown." |

### *In re § 2703(d) Order (2011)*

This was a petition by Twitter users to vacate the so-called Twitter Order granted by a federal court in Virginia upon the US government's *ex parte* motion. The Twitter Order required Twitter to provide the US government information relating to various Twitter accounts, including those of WikiLeaks, Julian Assange, and Bradley Manning. The motion to vacate the order was denied, but the motion to unseal one docket was granted.

| ITEM | NOTES |
|---|---|
| Case name: | Earlier case: *In re § 2703(d) Order* (2011).<br>Later case: *In re § 2703(d) Order* (2013). |
| Citation: | Earlier case: 830 F. Supp. 2d 114 (US District Court, Eastern District of Virginia, Alexandria Division) November 10, 2011.<br>Later case: No. 11-5151 (US Court of Appeals Fourth Circuit) January 25, 2013. |
| Jurisdiction: | Earlier case: United States District Court for the Eastern District of Virginia.<br>Later case: United States Court of Appeals, Fourth Circuit. |

| | |
|---|---|
| Main URL: | ACLU Virginia, *In re § 2703(d) Orders*, available at https://acluva.org/en/cases/re-ss2703d-orders.<br><br>Electronic Privacy Information Center, *In re Twitter Order Pursuant to 2703(d)* https://www.epic.org/amicus/twitter/wikileaks/.<br><br>Justia US Law, *In re: 2703(d) Application, No. 11-5151* (Fourth Cir. 2013) https://law.justia.com/cases/federal/appellate-courts/ca4/11-5151/11-5151-2013-01-25.html. |
| Charged with: | N/A (motion to vacate and motion to unseal) |
| Legislative provisions: | 18 U.S.C. section 2703(d) of the Stored Communications Act |
| Main target: | N/A (motion to vacate and motion to unseal sought) |
| Motivation: | Twitter's counsel argued before the US district court that the section 2703(d) order should be vacated on various grounds, such as arguing that the Twitter order violates their fourth amendment right to be free from unreasonable searches and seizures (i.e., disclosure of their IP address should be considered a "search" under the fourth amendment). Also, they argued that the Twitter order violates their constitutional right to procedural due process. As well, it was argued that the Twitter order violates their first amendment rights to free speech and association. Finally, they argued that the court should exercise discretion to deny the Twitter order to avoid the above-mentioned constitutional questions. |
| Convicted of: | N/A |
| Sentence: | N/A |
| Additional important information: | Motion to vacate denied, but motion to unseal granted on one docket. In an update to the case in 2013 at the US Court of Appeals for the Fourth Circuit: "Because the court found that there was no First Amendment right to access such documents, and the common law right to access such documents was presently outweighed by countervailing interests, the court denied the request for relief" (Justia).<br><br>Interesting expansion and appropriation of US constitutional notions of free speech and association, freedom from unreasonable search and seizure and of procedural due process. |

***United States of America v Dennis Collins, et al. ("PayPal 14")***

In December 2013, fourteen individuals connected with Anonymous were arrested in the United States for their alleged roles in cyber attacks against PayPal's website in 2010. The cyber attacks were in response to PayPal's suspension of payments to WikiLeaks and as part of a wider Anonymous campaign, "Operation Payback," which included "Operation Avenge Assange." Two additional individuals were arrested on similar charges.

| ITEM | NOTES |
|---|---|
| Case name: | *United States of America v. Dennis Collins, et al* (2011) |
| Citation: | No. CR 11-00471 DLJ |
| Jurisdiction: | United States District Court, Northern District of California, San Jose Division |
| Main URL: | FBI, "Sixteen Individuals Arrested in the United States for Alleged Roles in Cyber Attacks" (press release, July 19, 2011), available at http://www.fbi.gov/news/pressrel/press-releases/sixteen-individuals-arrested-in-the-united-states-for-alleged-roles-in-cyber-attacks (last accessed November 10, 2011).<br><br>US Attorney's Office, Northern District of California, "Thirteen Defendants Plead Guilty For December 2010 Cyber-Attack Against PayPal" (press release, December 6, 2013), available at http://www.justice.gov/usao/can/news/2013/2013_12_06_thirteen.guiltyplea.press.html.<br><br>D. Lucas, "Exclusive: The Legendary #Anonymous PayPal 14 Speak Out Post-Sentencing," *Cryptosphere*, October 31, 2014, available at https://thecryptosphere.com/2014/10/31/exclusive-the-anonymous-paypal-14-speak-out-post-sentencing/. |
| Charged with: | California charges: conspiracy and intentional damage to a protected computer.<br><br>For indictment, see http://ia600502.us.archive.org/24/items/gov.uscourts.cand.242989/gov.uscourts.cand.242989.1.0.pdf. |
| Legislative provisions: | 18 U.S.C. section 1030(b)(felony)—Conspiracy offence<br>18 U.S.C. section 1030(a)(5)(A)(misd.)—Intentional damage to a protected computer. |
| Main target: | DDoS attacks on PayPal |
| Motivation: | Retaliation against PayPal's termination of WikiLeaks's donation account |

| | |
|---|---|
| Convicted of: | With the exception of Valenzuela, Phillips, and Miles, each of the defendants pleaded guilty to one count of conspiracy, in violation of 18 U.S.C. section 1030(b)(felony), and one count of intentional damage to a protected computer, in violation of 18 U.S.C. section 1030(a)(5)(A) (misd.).<br><br>Defendant Valenzuela pleaded guilty to one count of reckless damage to a protected computer, in violation of 18 U.S.C. section 1030(a)(5)(A)(misd.).<br><br>Defendants Phillips and Miles pled guilty to one count each of intentional damage to a protected computer, in violation of 18 U.S.C. section 1030(a)(5)(A)(misd.) only. |
| Sentence: | In 2014, Collins was the only member charged with involvement with the PayPal 14 and Payback 13, but he was sentenced to house arrest for six months for health reasons.<br><br>Thirteen of the PayPal 14 of Anonymous had their felony charges reduced to a single misdemeanour and were sentenced to probation and $5,600 restitution. |
| Additional important information: | The individuals named in the San Jose indictment are:<br>• Dennis Collins, aka "Owen" and "Iowa;"<br>• Christopher Wayne Cooper, aka "Anthrophobic;"<br>• Joshua John Covelli, aka "Absolem" and "Toxic;"<br>• Keith Wilson Downey;<br>• Mercedes Renee Haefer, aka "No" and "MMMM;"<br>• Donald Husband, aka "Ananon;"<br>• Vincent Charles Kershaw, aka "Trivette," "Triv" and "Reaper;"<br>• Ethan Miles;<br>• James C. Murphy;<br>• Drew Alan Phillips, aka "Drew010;"<br>• Jeffrey Puglisi, aka "Jeffer," "Jefferp" and "Ji;"<br>• Daniel Sullivan;<br>• Tracy Ann Valenzuela; and<br>• Christopher Quang Vo.<br><br>Dennis Collins was the only member who was charged in relation to both PayPal 14 and Payback 13.<br><br>The chairman of eBay, Pierre Omidyar, called for leniency in the prosecution of those accused of playing a part in DDoS-ing PayPal. He pointed out that the accused were part of thousands who took part in the protest. |

### *United States of America v. Steiger*

This case concerns a hacker that obtained evidence that the defendant, Steiger, was producing and collecting child pornography, and passed the evidence to law enforcement in the United States. The issue in this case was whether "the evidence was obtained in violation of the Fourth Amendment as the hacker was a government agent."

| ITEM | NOTES |
|---|---|
| Case name: | *United States of America v. Steiger* (2003) |
| Citation: | 318 F. 3d 1039, Nos. 01-15788, 01-16100 and 01-16269 (January 14, 2003) |
| Jurisdiction: | United States Court of Appeals, Eleventh Circuit |
| Main URL: | Case: Available at http://scholar.google.com.au/scholar_case?case=5611821785646747519 |
| Charged with: | Hacker not charged as he was not being prosecuted. The hacker in question was from Turkey. He was merely the source of the information about Stieger's sexual abuse of a young child in the United States |
| Legislative provisions: | The fourth amendment (right against unreasonable searches and seizures) |
| Main target: | Steiger—producer and possessor of child pornography |
| Motivation: | To help law-enforcement officers catch child predators |
| Convicted of: | N/A |
| Sentence: | N/A |
| Additional important information: | For a search by a private person to implicate the fourth amendment, the person must act as an instrument or agent of the government.[1]<br><br>In 2006, the defendant attempted to convince the court of a motion for a new trial, but failed. As a result, the 2003 judgment still stands (see https://www.gpo.gov/fdsys/pkg/USCOURTS-almd-2_00-cr-00170/pdf/USCOURTS-almd-2_00-cr-00170-0.pdf). |

### *United States of America v. Jarrett*

This case concerns a hacker that obtained evidence that the defendant was producing and collecting child pornography, and passed the evidence to law enforcement in the United States. The issue in this case was "whether evidence obtained by a hacker and used in a prosecution implicates the 4th amendment, and there has been communication between the hacker and law enforcement about the evidence."

| ITEM | NOTES |
|---|---|
| Case name: | *United States of America v. Jarrett* |
| Citation: | 338 F. 3d 339, No. 02-4953 (July 29, 2003) |
| Jurisdiction: | United States Court of Appeals, Fourth Circuit |
| Main URL: | Case: http://scholar.google.com.au/scholar_case?case=7704360326371177621 |
| Charged with: | Hacker not charged as he was not being prosecuted in the United States |
| Legislative provisions: | The fourth amendment (right against unreasonable searches and seizures) |
| Main target: | Jarrett—producer and possessor of child pornography |
| Motivation: | To help law-enforcement officers catch child predators |
| Convicted of: | N/A |
| Sentence: | N/A |
| Additional important information: | Whether the hacker's search was a government search turns on "(1) whether the Government knew of and acquiesced in the private search; and (2) whether the private individual intended to assist law enforcement or had some other independent motivation" (*United States of America v. Jarrett*). There must be more than knowledge or acquiescence—there must be participation or affirmative encouragement. |

***United States of America v. Raynaldo Rivera***

Raynaldo Rivera, of Tempe, Arizona—who allegedly used the online nicknames of "neuron," "royal" and "wildciv"—surrendered to police in Phoenix six days after a federal grand jury in Los Angeles produced an indictment accusing Rivera and co-conspirators of stealing information from Sony Pictures Europe's computer systems in May and June 2011 using an SQL injection attack. The SQL injection attack exploits flaws in the handing of data input for databases to take control of a system—in this case, against the studio's website. The indictment says Rivera helped to post the confidential information onto LulzSec's website and announced the intrusion via the hacking group's Twitter account.

| ITEM | NOTES |
|---|---|
| Case name: | *United States of America v. Raynaldo Rivera* |
| Citation: | CR No. 12- 798-JAK |
| Jurisdiction: | United States District Court for the Central District of California |
| Main URL: | C. Arthur, "LulzSec Hacker Arrested Over Sony Attack," *Guardian*, August 29, 2012, available at http://www.guardian.co.uk/technology/2012/aug/29/lulzsec-hacker-arrest-sony-attack.<br><br>Plea agreement, *FreeAnons* https://freeanons.org/wp-content/uploads/court-documents/Raynaldo-Rivera.pdf.<br><br>FBI, "Second Member of Hacking Group Sentenced to More Than a Year in Prison for Stealing Customer Information from Sony Pictures Computers" (FBI press release, August 8, 2013), available at https://archives.fbi.gov/archives/losangeles/press-releases/2013/second-member-of-hacking-group-sentenced-to-more-than-a-year-in-prison-for-stealing-customer-information-from-sony-pictures-computers. |
| Charged with: | Conspiracy and intent to cause damage without authorization to a protected computer |
| Legislative provisions: | 18 U.S.C. sections 371 and 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(I) |
| Main target: | Sony Pictures Europe's computer systems |
| Motivation: | Unknown, perhaps for the "lulz" |
| Convicted of: | Conspiracy and intent to cause damage without authorization to a protected computer |
| Sentence: | Rivera initially faced fifteen years in prison. However, after striking a plea deal, he was sentenced to one year and one day in federal prison by United States District Judge John A. Kronstadt. Rivera was also ordered to serve thirteen months of home detention, to perform 1,000 hours of community service and to pay $605,663 in restitution to Sony Pictures. |
| Additional important information: | Following the Sony Pictures Europe breach, LulzSec published the names, birth dates, addresses, emails, phone numbers, and passwords of thousands of people who had entered contests promoted by Sony, and publicly boasted of its exploits. |

| | |
|---|---|
| | LulzSec released a statement related to the Sony hack. LulzSec said: "From a single injection we accessed EVERYTHING," the hackers said in a statement at the time. "Why do you put such faith in a company that allows itself to become open to these simple attacks?"<br><br>A number of arrests followed in the United Kingdom, where six people have been charged with various offences linked to LulzSec's activities.<br><br>An accused British hacker, Ryan Cleary, was indicted by a US grand jury on charges related to LulzSec attacks on several media companies, including Sony Pictures.<br><br>Cody Kretsinger, who pleaded guilty to the same two charges Rivera faced, was sentenced to one year in federal prison, one year of home detention after the completion of his prison sentence, a fine of $605,663 in restitution to Sony Pictures and 1,000 hours of community service.<br><br>Hector Xavier Monsegur, a Puerto Rican living in New York, pled guilty to 12 charges, including three of conspiracy to hack into computers, five of hacking, one of hacking for fraudulent purposes, one of conspiracy to commit bank fraud, and one of aggravated identity theft.<br><br>Those charges would attract a total of 124 years in jail, but he arranged a plea bargain with the US government. Monsegur received a six-month reprieve from sentencing in light of his cooperation with the government.<br><br>Monsegur, a hacker turned FBI informant, provided the FBI with details enabling the arrest of five other hackers associated with the groups Anonymous, LulzSec and AntiSec.<br><br>A court filing made by prosecutors in late May 2014 revealed Monsegur had prevented 300 cyber-attacks in the three years since 2011, including planned attacks on NASA, the US military and media companies.<br><br>Monsegur served seven months in prison after his arrest but had been free since then while awaiting sentencing. At his sentencing on May 27, 2014, he was given "time served" for co-operating with the FBI and set free under one year of parole. |

### *Aaron Swartz*

Aaron Swartz was facing up to thirty-five years in jail for illegally downloading 4.8 million articles from the JSTOR database in 2011. The Massachusetts Institute of Technology (MIT), whose data network was used in the hack, valued the downloaded information at $50,000. Aaron strongly believed that information, and especially research, should be public and free. Faced with the harsh prison sentence and under the pressure of legal fees, Aaron committed suicide at his home on January 11, 2013.

| ITEM | NOTES |
|---|---|
| Case name: | *United States of America v. Aaron Swartz* |
| Citation: | 1:11-cr-10260 |
| Jurisdiction: | United States District Court for the District of Massachusetts |
| Main URL: | S. Farberov, H. Pow, and J. Nye, "Revealed: Prosecutors turned down Reddit co-founder Aaron Swartz's request for plea deal over MIT hacking case TWO DAYS before his suicide," *Daily Mail*, January 14, 2013, available at http://www.dailymail.co.uk/news/article-2262137/Aaron-Swartz-Reddit-founder-request-plea-deal-turned-Massachusetts-prosecutor.html#axzz2KkIHBHh6 |
| Charged with: | Thirteen counts of felony hacking including wire fraud, computer fraud, and unlawfully obtaining information from a protected computer |
| Legislative provisions: | 18 U.S.C. sections 1343, 1030(a)(4), 1030(a)(2), 1030(a)(5)(B), and 2 |
| Main target: | JSTOR database |
| Motivation: | Swartz believed that academic articles funded by taxpayers' money should be made available for free |
| Convicted of: | Charges were dismissed following Swartz's death |
| Sentence: | Faced up to thirty-five years in jail and millions of dollars in fines |
| Additional important information: | In 2010, Swartz allegedly connected a laptop to MIT's systems through a basement network wiring cupboard. He registered as a guest under the fictitious name, Gary Host—a hacking in-joke in which the first initial and last name spell "ghost." He then used a software program to "rapidly download an extraordinary volume of articles from JSTOR," according to the indictment. |

| | |
|---|---|
| | In the following months, MIT and JSTOR tried to block the recurring and massive downloads, on occasion denying all MIT users access to JSTOR. However, Swartz allegedly got around it, in part, by disguising the computer source of the demands for data.<br><br>It is alleged that on January 6, 2011, Swartz went to the wiring closet to remove the laptop, attempting to shield his identity by holding a bike helmet in front of his face and seeing his way through its ventilation holes. He fled when MIT police tried to question him that day, it is claimed. Legal proceedings followed. |

***Lauri Love (British) AKA "nsh" "route" "peace" "LOVE"***

British citizen Lauri Love is charged with hacking charges in the United States. He is accused of hacking US government departments—stealing the personal details of 5,000 servicemen and women and classified US data by installing hidden "shells" or back doors within the networks.

| ITEM | NOTES |
|---|---|
| Case name: | *Lauri Love v. the Government of the United States of America* |
| Citation: | [2018] EWHC 172 |
| Jurisdiction: | 2013: United States District Court of New Jersey<br>2014: United States Southern District Court of New York and Eastern District of Virginia<br>2018: High Court of England and Wales |
| Main URL: | J. Halliday, "Briton Lauri Love faces hacking charges in US," *Guardian*, October 29, 2013, available at http://www.theguardian.com/world/2013/oct/28/us-briton-hacking-charges-nasa-lauri-love.<br><br>BBC News, "Lauri Love case: Hacking Suspect Wins Extradition Appeal," February 5, 2018, available at https://www.bbc.com/news/uk-england-42946540.<br><br>Indictment, https://www.scribd.com/doc/179595899/Love-Lauri-Indictment.<br><br>Case (High Court of England and Wales), https://freelauri.com/wp-content/uploads/2018/02/lauri-love-v-usa.pdf.<br><br>D. Pauli, "Aussies Hacked Pentagon, US Army, and Others," IT News, October 29, 2013, available at https://www.itnews.com.au/news/aussies-hacked-pentagon-us-army-and-others-362202. |

| | |
|---|---|
| Charged with: | Violation of 18 U.S.C. sections 371, 1030, and 2 |
| Legislative provisions: | Computer Fraud and Abuse Act, 18 U.S.C. sections 371, 1030, and 2 |
| Main target: | Classified US data—US Army, the Environmental Protection Agency, and NASA |
| Motivation: | Prosecutors alleged that Love told a colleague in one exchange over IRC: "You have no idea how much we can fuck with the US government if we wanted to…I think we can do some hilarious stuff" |
| Convicted of: | Love is under indictment in the United States related to a violation of the Computer Fraud and Abuse Act. In 2018, the High Court of England and Wales ruled against extraditing Love to the United States to face trial. |
| Sentence: | If extradited to the United States, Love would have faced up to ten years' prison time and a fine of $250,000 if found guilty. |
| Additional important information: | Selected methods of hacking:<br>• Internet Protocol<br>• SQL<br>• SQL Injection Attacks<br>• SQL Injection Strings<br>• HTML<br>• Malware<br>• "Coldfusion" (is a web application and development platform that uses a programming language also referred to as Coldfusion. Adobe later purchased Coldfusion. Coldfusion hacks are those which use the platform to obtain unauthorised access to the backend of a website).<br>• Proxy servers—Used to conceal hacks<br>• IRC<br><br>"Collectively, the hacks described herein substantially impaired the functioning of dozens of computer servers and resulted in millions of dollars of damages to the Government Victims," US prosecutors claimed (as per IT News).<br><br>In February 2018, the High Court of England and Wales ruled that Love would not be extradited to the United States to face trial. |

### *Jeremy Hammond AKA "yohoho," "tylerknowsthis," "sup_g," "Anarchaos," "POW," "crediblethreat," "burn," "ghost," "anarchacker" (LulzSec, AntiSec)*

Jeremy Hammond leaked millions of emails by Stratfor to WikiLeaks. The emails revealed disturbing evidence of the corruption behind Stratfor, including insider trading techniques, coercive methods, and off-shore share structures (details below).

| ITEM | NOTES |
|---|---|
| Case name: | *United States of America v. Jeremy Hammond* |
| Citation: | 12 Cr. 185 (LAP) (2013) |
| Jurisdiction: | United States, District Court—Southern District of New York |
| Main URL: | Case, http://www.justice.gov/usao/nys/pressreleases/May13/HammondJeremyPleaPR/U.S.%20v.%20Jeremy%20Hammond%20S2%20Information.pdf.<br><br>Additional legal documents related to Hammond's case, https://freejeremy.net/category/legal/.<br><br>WikiLeaks, "The Gifiles," https://wikileaks.org/the-gifiles.html.<br><br>J. Kopstein, "Hacker with a cause," *New Yorker*, November 21, 2013, available at http://www.newyorker.com/online/blogs/elements/2013/11/jeremy-hammond-and-anonymous-hacker-with-a-cause.html.<br><br>E. Pilkington, "Jeremy Hammond: FBI directed my attacks on foreign government sites,'" *Guardian*, November 16, 2013, available at http://www.theguardian.com/world/2013/nov/15/jeremy-hammond-fbi-directed-attacks-foreign-government. |
| Charged with: | He was indicted on six counts, but pled guilty to one: conspiracy to violate the Computer Fraud and Abuse Act.<br><br>The six counts did not come to court, but are worth mentioning.<br><br>Count 1: Conspiracy to commit computer hacking.<br>Count 2: Conspiracy to commit computer hacking—LulzSec. In violation of 18 U.S.C. section 1030(b)—relevant to the cyber attack in June 2011 on computer systems used by the Arizona Department of Public Safety. |

| | |
|---|---|
| | Counts three, four, five, and six: other counts of conspiracy to commit computer hacking in violation of 18 U.S.C. section 1030(b) and substantive computer hacking in violation of sections 1030(a)(5)(A), 1030(b), and 1030(c)(4)(B)(i). Also, conspiracy to commit access device fraud in violation of section 1029(b)(2) and aggravated identity theft in violation of sections 1028A and (2).<br><br>Counts three, four, five, and six are all related to the "Stratfor hack" (discussed below). |
| Legislative provisions: | Computer Fraud and Abuse Act |
| Main target: | Stratfor |
| Motivation: | Corruption of Stratfor, including bribery, insider trading, and corrupt connections with large corporations and government agencies.<br><br>Hammond's sentencing transcript revealed his motivation: "I felt I had an obligation to use my skills to expose and confront injustice—and to bring the truth to light…I have tried everything from voting petitions to peaceful protest and have found that those in power do not want the truth exposed.... We are confronting a power structure that does not respect its own systems of checks and balances, never mind the rights of its own citizens or the international community." |
| Convicted of: | Pled guilty to conspiracy |
| Sentence: | Ten years' imprisonment with three years' supervised release |
| Additional important information: | Counsel for the defendant: Elizabeth Fink US; plaintiff: represented by Rosemary Nidiry, Thomas G. A. Brown<br>Judges: Loretta A. Preska (Chief United States District Judge)<br><br>Note: Preska's husband's email had been leaked with the Stratfor information.<br><br>Hammond also claims that former hacker turned FBI informant, Hector Xavier Monsegur (aka "Sabu"), directed him to attack several government websites. |

### *Anonymous and St0rmyw0rm*

Anonymous claims to have temporarily shut down the National Surveillance Agency (NSA) website for hours through a DDoS attack. Both Anonymous and St0rmyw0rm have claimed to have stolen the email addresses of at least 400 NSA workers and sent them "troll" messages.

| ITEM | NOTES |
|---|---|
| Case name: | N/A |
| Citation: | N/A |
| Jurisdiction: | United States |
| Main URL: | RT, "NSA Site went down due to "internal errors," not DDoS attack, agency claims," October 27, 2013, available at http://rt.com/usa/nsa-site-ddos-attack-754/.<br><br>E. Kovacs, "NSA Website Disrupted Following PRISM Leak, Hackers Want to Troll Agency," Softpedia, June 12, 2013, available at https://news.softpedia.com/news/NSA-Website-Disrupted-Following-PRISM-Leak-Hackers-Want-to-Troll-Agency-360574.shtml. |
| Charged with: | N/A |
| Legislative provisions: | Computer Fraud and Abuse Act |
| Main target: | National Surveillance Agency |
| Motivation: | Unknown, but it could be to deter the United States from future illegal surveillance |
| Convicted of: | N/A |
| Sentence: | N/A |
| Additional important information: | The NSA claims that an 'internal error', not a DDoS attack, was responsible for the temporary shutdown of their website. |

### *Paracha v. Obama*

This case was about an application for immediate access to all publicly available WikiLeaks documents relevant to the petitioner's case. The government opposed the application because there was no emergency, otherwise a requirement for immediate access.

| ITEM | NOTES |
|---|---|
| Case name: | *Paracha v. Obama* (2011) |
| Citation: | No. 04-2022 (PLF) (April 29, 2011). |
| Jurisdiction: | United States District Court, District of Columbia |
| Main URL: | Court order related to the documents, https://scholar.google.com.au/scholar_case?case=7165402973414950017&q=Paracha+wikileaks&hl=en&as_sdt=2006&as_vis=1#r[1].<br><br>Petitioner's (Paracha's) emergency application, https://fas.org/sgp/jud/par/042711-access.pdf.<br><br>Respondents' (Obama et al.'s) response, https://fas.org/sgp/jud/par/061511-response376.pdf. |
| Cause of action: | Opposition by government of application for immediate access to all publicly available WikiLeaks documents relevant to Saifullah<br>Paracha's case. (The petitioner was a detainee at Guantanamo Bay). |
| Legislative provisions: | To determine whether an emergency application for immediate access to WikiLeaks documents relevant to Paracha's case is to be granted, the court considered: Executive Order 13,526, section l.1(c) and case law |
| Main target: | WikiLeaks targeted the US government's confidential files on Guantanamo Bay detention camp detainees. Paracha's counsel wanted access to the documents. |
| Motivation: | WikiLeaks sought to shine the light of truth on former US President George W. Bush's "war on terror" campaign by seeking to expose files held by the US government on its detainees at Guantanamo Bay. Paracha's counsel filed an emergency application for immediate access to all available WikiLeaks documents relevant to his case. |
| Convicted of: | Paracha was convicted in 2005 of providing support to al-Qaeda. The case involved an emergency application for immediate access to all publicly available WikiLeaks documents relevant to his case. |
| Sentence: | The US government opposed Paracha's application because there was no emergency, which is a requirement for immediate access. Also, the US government held that the leaked WikiLeaks documents are to remain classified by the law. Paracha was also denied approval for transfer in April 2016. |

| | |
|---|---|
| Additional important information: | "The Court sees no need for an expedited schedule because...no emergency exists in this litigation, which has been continued pending Mr. Paracha's filing of a status report that was due by April 1, 2011 but has still not been filed" (*Paracha v. Obama*).<br><br>The Justice Department's Court Security Office said that the publicly available WikiLeaks documents remain classified by law. |

### *Bank Julius Baer & Co. Ltd. v. WikiLeaks*

This case concerned an allegation that WikiLeaks "had wrongfully published on a website confidential, as well as forged, bank documents belonging to plaintiffs." The court dissolved a previously issued permanent injunction and denied a request for a preliminary injunction (against publication).

| ITEM | NOTES |
|---|---|
| Case name: | *Bank Julius Baer & Co. Ltd. v. WikiLeaks* |
| Citation: | No. C 08-00824 JSW (February 29, 2008) |
| Jurisdiction: | United States District Court, Northern District of California |
| Main URL: | Case provided by the Electronic Frontiers Foundation at https://www.eff.org/files/filenode/baer_v_wikileaks/wikileaks102.pdf<br><br>ACLU Northern California, *Bank Julius Baer & Co. Ltd. v. WikiLeaks* (March 6, 2008) https://www.aclunc.org/our-work/legal-docket/bank-julius-baer-co-ltd-v-wikileaks. |
| Causes of action: | Unlawful and unfair business practices, declaratory relief, interference with contract, interference with prospective economic advantage, conversion, and injunctive relief |
| Legislative provisions: | California Business and Professions Code section 17200 and the first amendment |
| Main target: | It is alleged that a former Baer employee stole and leaked client data. WikiLeaks published it. |
| Motivation: | WikiLeaks published leaked documents that exposed off-shore tax evasion and money laundering by Baer's wealthy clients |
| Convicted of: | N/A |
| Sentence: | N/A |

| | |
|---|---|
| Additional important information: | Initially, Baer obtained a permanent injunction against the domain registrar Dynadot, LLC, shutting down the domain name wikileaks.org. However, the American Civil Liberties Union (ACLU), the Electronic Frontier Foundation (EFF), and others filed a motion to intervene the injunction and they were successful. The ACLU and EFF persuaded the court to dissolve an order that sought to take down the domain name wikileaks.org.<br><br>The court held that (1) it might not have had jurisdiction over the injunction due to the nature of the plaintiffs (some being foreign citizens and entities) and their varying physical addresses; (2) the injunction could impede on free speech under the first amendment to the United States Constitution; (3) the injunction that was issued had the opposite effect as was intended; and (4) the plaintiffs did not adequately show that the injunction would serve its intended purpose.<br><br>The bank abandoned the case on March 5, 2008. |

## THE UNITED KINGDOM

### *"Kayla" aka Ryan Ackroyd*

"Kayla" is the handle of Ryan Ackroyd, one of the core members of LulzSec involved in a series of cyber attacks, from May 6 to June 26, 2011, dubbed 50 Days of Lulz. Kayla was responsible for hacking into multiple military and government websites, as well as the networks of Gawker in December 2010, HBGary in 2011, PBS, Sony, Infragard Atlanta, Fox Entertainment, and more.

| ITEM | NOTES |
|---|---|
| Case name: | *R v Cleary, Davis, Al-Bassam and Ackroyd* |
| Citation: | Southwark Crown Court (May 16 and 24, 2013) |
| Jurisdiction: | United Kingdom, Southwark Crown Court in London |
| Main URL: | Free Anons, "Interview: Ryan Ackroyd AKA Kayla of LulzSec" (April 15, 2014) https://freeanons.org/interview-ryan-ackroyd-aka-kayla-lulzsec/.<br><br>S. Storm, "London court: LulzSec hackers called 'latter day pirates' at 'cutting-edge' of cybercrime," *Computer World*, May 15, 2013, available at https://www.computerworld.com/article/2475432/cybercrime-hacking/london-court--lulzsec-hackers-called--latter-day-pirates--at--cutting-edge--of-cy.html. |

| | |
|---|---|
| Charged with: | Implied to be offences under Computer Misuse Act 1990 (with which others arrested in similar circumstances were charged) |
| Legislative provisions: | Computer Misuse Act 1990 section 3—unauthorized act to impair the operation of a computer |
| Main target: | Military and government, as well as large multinational companies |
| Motivation: | It has been suggested that LulzSec sought to achieve international notoriety and publicity (see Storm) |
| Convicted of: | April 9, 2013: Pled not guilty to DDoS attacks that were carried out under the LulzSec banner during its AntiSec campaign (discussed below). However, Ackroyd did plead guilty to violating the Computer Misuse Act (unauthorized act to impair the operation of a computer). |
| Sentence: | In 2013, Ackroyd was sentenced to a thirty-month prison sentence in England, but was released on a "home detention curfew" after serving ten months. He was on probation until 2015 and under a "serious crime prevention order," which prevented him from using encryption that allows hidden volumes, virtual machines, or from deleting his web history. |
| Additional important information: | In the case, Cleary and the other defendants (Davis, Al-Bassam, Ackroyd) all pled guilty to two counts of conspiracy to commit unauthorized act with the intent to impair the operation of a computer and unauthorized access and modification to websites.<br><br>Ryan Ackroyd is now an associate lecturer at Sheffield Hallam University. |

***R v Weatherhead, Rhodes, Gibson and Birchall***

Christopher Weatherhead ("Nerdo")—had a leading role in plotting the attacks.

Ashley Rhodes ("Nikonelite")—was the most "hands-on" of the four men and the only one with DDoS software on his computer.

Peter Gibson—played a lesser role in the attacks.

Jake Birchall ("Fennic")—conspired to impair the operation of computers during the attacks. Birchall was said to have a "great deal or organisational control" over "AnonOps." His sentence was handed down at a later date, once he turned eighteen.

The four men were each convicted of attacking anti-piracy and financial companies between August 2010 and January 2011. The assaults on PayPal, Visa, and MasterCard were in retaliation for those companies cutting ties with the whistle-blowing website WikiLeaks following its release of secret diplomatic cables.

| ITEM | NOTES |
|---|---|
| Case name: | *R v Christopher Weatherhead, Ashley Rhodes, Peter Gibson, and Jake Birchall* |
| Citation: | Southwark Crown Court (January 24, 2013) |
| Jurisdiction: | United Kingdom, Southwark Crown Court in London |
| Main URL: | J. Halliday, "Anonymous Teenager Hacker Spared Jail over Cyber Attacks," *Guardian*, February 1, 2013, available at http://www.guardian.co.uk/technology/2013/feb/01/anonymous-teenage-hacker |
| Charged with: | DDoS on Paypal, Visa, and Mastercard in December 2010 |
| Legislative provisions: | Computer Misuse Act 1990, section 3—unauthorized acts with intent to impair; conspiring to impair the operation of computers |
| Main target: | PayPal, Visa, MasterCard |
| Motivation: | In retaliation for companies cutting ties with the whistle-blowing website WikiLeaks following its release of secret US diplomatic cables |
| Convicted of: | Attacking anti-piracy and financial companies via DDoS attacks between August 2010 and January 2011.<br><br>Weatherhead, Rhodes, and Gibson were convicted of one count each of conspiracy to impair the operation of computers (Rhodes and Gibson pled guilty). |
| Sentence: | Christopher Weatherhead: eighteen months in prison.<br>Ashley Rhodes: seven months in prison.<br>Peter Gibson: six month suspended sentence.<br>Jake Birchall: eighteen-month youth rehabilitation order and a sixty-hours unpaid work. |
| Additional important information: | PayPal was repeatedly attacked in December 2010 after the website decided not to process payments made to the Wau Holland Foundation (an organization involved in raising funds for WikiLeaks).<br><br>During trial, prosecutors said the attack had cost PayPal $5.5 million in loss of trading as well as in software and hardware updates to fend off similar attacks.<br><br>Birchall was told he would have been imprisoned had he not been sixteen at time of the offence |

### *R v Glenn Mangham*

Glenn Mangham impersonated an employee of the social-networking site Facebook while on holiday and hacked into three of its servers. Using the code name "Gamma Ray" he stole the secret computer code "that gives Facebook its value" and downloaded it to his home computer's hard drive. Mangham claimed that his work was "ethical hacking" and he breached the security so that he could identify vulnerabilities within the site, which the developers could then strengthen.

| ITEM | NOTES |
|---|---|
| Case name: | *R v Glenn Steven Mangham.*<br>Court of Appeal: *R v Glenn Steven Mangham* |
| Citation: | Southwark Crown Court (February 17, 2012)<br>Court of Appeal [2012] EWCA Crim 973 (April 4, 2012) |
| Jurisdiction: | United Kingdom, Southwark Crown Court in London; England and Wales Court of Appeal (Criminal Division) |
| Main URL: | E. Protalinski, "British student jailed for hacking into Facebook," *Zdnet*, February 18, 2012, available at http://www.zdnet.com/blog/facebook/british-student-jailed-for-hacking-into-facebook/9244 (last accessed December 21, 2016).<br><br>M. Mangham, "The Facebook Hack: What Really Happened" on *GMangham Blog* (April 23, 2012), available at http://gmangham.blogspot.co.uk/2012/04/facebook-hack-what-really-happened.html (last accessed December 21, 2016).<br><br>Case (Court of Appeal), http://www.bailii.org/ew/cases/EWCA/Crim/2012/973.html. |
| Charged with: | Three counts of unauthorized access and modification of a computer but he was convicted of two counts under the Computer Misuse Act 1990 |
| Legislative provisions: | Computer Misuse Act 1990, sections 1 (unauthorized access), 3 (unauthorized acts with intent to impair a protected computer), and 3A (making, supplying or obtaining articles for use in offences under sections 1or 3) |
| Main target: | Facebook |
| Motivation: | Ethical hacking to identify site vulnerabilities |

| | |
|---|---|
| Convicted of: | Mangham pleaded guilty to four counts: counts one to three, securing unauthorized access to computer material with intent (contrary to the Computer Misuse Act 1990, section 1) and count four, the unauthorized modification of computer material, contrary to section 3 of that act |
| Sentence: | Was initially sentenced to eight months' imprisonment and was handed a "serious crime prevention" order, which restricted his access to the internet and forfeiture of computer. Later, the appeal was allowed and the sentence was reduced to four months' imprisonment, with the order quashed. |
| Additional important information: | The presiding judge told Mangham: "This was not just a bit of harmless experimentation—you accessed the very heart of the system of an international business of massive size."<br><br>Mangham claimed he was an ethical hacker who had previously helped Yahoo improve its security and had wanted to do the same for Facebook. |

## AUSTRALIA

### *Matthew George*

Matthew George was an Australian member of Anonymous who participated in what the group called Operation Titstorm. He was charged with inciting others to attack government websites and the magistrate likened his activities to cyber terrorism.

| ITEM | NOTES |
|---|---|
| Case name: | Court case unreported online. Case details retrieved from news articles. |
| Citation: | Court case unreported online. Case details retrieved from news articles. |
| Jurisdiction: | Australia, Newcastle Local Court |
| Main URL: | S. Whyte. "Meet the Hacktivist Who Tried to Take Down the Government," *Sydney Morning Herald*, March 14, 2011, available at https://www.smh.com.au/technology/meet-the-hacktivist-who-tried-to-take-down-the-government-20110314-1btkt.html (last accessed November 7, 2011). |
| Charged with: | Unauthorized impairment of electronic communication to or from a Commonwealth computer |
| Legislative provisions: | Criminal Code Act 1995 section 477.3—unauthorized impairment of electronic communication |

| | |
|---|---|
| Main target: | Denial-of-service attack against the websites of the prime minister and a cabinet minister in protest of proposed Internet filtering and the presence of certain URLs on a proposed blacklist |
| Motivation: | Protest Internet filtering |
| Convicted of: | Unauthorized impairment of electronic communication to or from a Commonwealth computer |
| Sentence: | $550 fine |
| Additional important information: | Another Anonymous member involved in the attack was Steve Slayo, who faced a good behaviour bond for the offence—the magistrate did not record a conviction for his offence. |

### *Justin Michael Soyke*

Australian teenage member of Anonymous, Justin Michael Soyke, aka "Juzzy" and "Absantos," received a three-year sentence for attempting to hack government and company servers. He was able to gain system and website administrator privileges, hence, accessing private information. The Commonwealth Director of Public Prosecutions claimed that it was likely that Soyke engaged with other hackers to perform the attack.

| ITEM | NOTES |
|---|---|
| Case name: | Initial court case unreported online<br>Criminal appeal case reported online: *Soyke v R* |
| Citation: | [2016] NSWCCA 112 (June 10, 2016) |
| Jurisdiction: | Australia, New South Wales Court |
| Main URL: | J. Saarinen, "Aussie Anon sentenced to three years' prison," IT News, November 19, 2015, available at https://www.itnews.com.au/news/aussie-anon-sentenced-to-three-years-prison-411978. |
| Charged with: | One count of unauthorized modification of computer data, in violation of Criminal Code Act 1995 section 477.2(1), one count of attempt to cause unauthorized modification of computer data, in violation of sections 477.2(1) and 11.1, and two counts of unauthorized access to data with intent to commit serious offence, in violation of section 466.1(1)(a)(i). Each carry a maximum penalty of ten years' imprisonment. |

| | |
|---|---|
| | Another seventeen offences of attempt to cause unauthorized access to restricted data under sections 478.1(1) and 11.1(1) of the code, which each carry maximum penalties of two years' imprisonment, were also taken into account. |
| Legislative provisions: | Criminal Code Act 1995 sections 477, 478.1(1), and 11.1(1) |
| Main target: | Government and company servers |
| Motivation: | Unknown, but believed to be in connection with Anonymous efforts to make information about corporations and governments publicly available |
| Convicted of: | One count of unauthorized modification of computer data, in violation of Criminal Code Act 1995 section 477.2(1); one count of attempt to cause unauthorized modification of computer data, in violation of sections 477.2(1) and 11.1; and two counts of unauthorized access to data with intent to commit serious offence, in violation of section 466.1(1)(a)(i).<br><br>A further seventeen offences of attempt to cause unauthorized access to restricted data in violation of sections 478.1(1) and 11.1(1) were also taken into account. |
| Sentence: | October 15, 2015: Soyke was sentenced on twenty-one charges of computer hacking, with three years' imprisonment and an order that he be released on recognizance of $5,000 to be of good behaviour after serving twelve months.<br>June 10, 2016: Soyke's appeal was dismissed. |
| Additional important information: | Soyke is linked to other hackers associated with Anonymous such as UK citizen Lauri Love, and two other Australians, Mathew Hutchison (aka "Rax") and Adam John Bennett (aka "Lorax"). Love, Hutchison, and Bennett have also faced legal consequences because of their involvement with Anonymous. |

### *Anonymous Indonesia and BlackSinChan*

In retaliation to the spying scandal conducted by the Australian government against Indonesian officials, including former Indonesian Prime Minister Susilo Bambag Yudhoyono, various Indonesian hacking groups targeted Australian law-enforcement websites. The attacks also targeted groups that were not involved with the spying scandal, including the Reserve Bank of Australia (RBA)—sparking threats from Anonymous Australia. At the time, concerns developed around the potential of cyberwarfare emerging between Anonymous Australia and Anonymous Indonesia.

| ITEM | NOTES |
|---|---|
| Case name: | Unable to retrieve the case. Facts taken from news articles |
| Citation: | Unknown—unable to retrieve case |
| Jurisdiction: | Difficult to determine as both countries claim sovereignty. However, since the crime was conducted against Australia, this would be a federal offence |
| Main URL: | A. Coyne, "How the AFP nabbed an Aussie Anonymous hacker," It News, March 20, 2017, available at https://www.itnews.com.au/news/how-the-afp-nabbed-an-aussie-anonymous-hacker-455142.<br><br>M. Ross, "Anonymous Indonesia hacker says RBA, AFP attacks were retaliation for spying scandal," ABC News, November 21, 2013, available at http://www.abc.net.au/news/2013-11-21/hacker-says-rba-afp-attacks-were-retaliation-for-spying-scandal/5108220.<br><br>P. Smith, "Indonesian claims responsibility for RBA and AFP attack," *Australian Financial Review*, November 21, 2013, available at http://www.afr.com/p/technology/indonesian_claims_responsibility_Y8kgaLtlfixvXGV5V6FH3I.<br><br>W. Ockenden, "Crime Stoppers website hacked, police email addresses published in spying scandal 'payback,'" ABC News, November 27, 2013, available at http://www.abc.net.au/news/2013-11-26/crime-stoppers-site-targeted-by-indonesian-hackers/5116856. |
| Charged with: | Again, the constraints concerning the cooperation between Australia and Indonesia hindered the ability for law enforcement to charge individuals of a crime. Furthermore, it is difficult to charge a collective with a crime when not all its members were responsible for the hacks. |
| Legislative provisions: | Criminal Code Act 1995—Part 10.7 Computer Offences |
| Main target: | Over 150 Australian websites, including those of the RBA, AFP, ASIS, and Crime Stoppers. Targeted websites were mainly law-enforcement sites, which Anonymous Indonesia deemed as "important" to Australia. |
| Motivation: | Retaliation to Australian spying scandal of Indonesian officials. Revenge and deterrence. |
| Convicted of: | It is unknown what legal action was taken in response to Anonymous Indonesia and Anonymous Australia, but some Australian hackers were convicted and sentenced for their attacks against Australian websites. |

| | |
|---|---|
| | Australian hacker, Justin Michael Soyke (aka "Juzzy and Absantos") was charged with sixty out of an alleged 300 offences related to the attack on government websites. Soyke pled guilty to twenty-one charges of computer hacking.<br><br>Another two Australian hackers, Adam John Bennett (aka "Lorax") and Michael John Hutchison (aka "Rax"), were also charged. Bennett was convicted of six charges including aiding another person to cause the unauthorized impairment of electronic communications. Hutchison pled guilty to inciting others to commit an offence and to possessing a prohibited weapon. |
| Sentence: | Again, it is unknown what legal action was taken in response to Anonymous Indonesia and Anonymous Australia, but the three Australian hackers were sentenced. In October 2015, Soyke was sentenced to one year in jail and a three-year recognizance. In March 2016, Bennett was sentenced to two years' suspended imprisonment, 200 hours of community service, and an intensive supervision order. Hutchison entered guilty pleas for inciting others to commit an offence and to possessing a prohibited weapon. |
| Additional important information: | Many of the government groups that were targeted, such as the RBA, had nothing to do with the spying scandal. At the time, Anonymous Australia threatened to retaliate against Anonymous Indonesia if another hack against an innocent site were to be conducted. |

## CANADA

### *Rehtaeh Parsons Rape Case*

Canadian teenager Rehtaeh Parsons was gang raped when she was fifteen. The rapists circulated a digital image of the rape, which was shared on the Internet. Parsons committed suicide after facing years of constant torment and related bullying. The Royal Canadian Mounted Police (RCMP) investigated the for a year but said it did not have sufficient evidence to lay charges. This outraged people all over the Internet, including Anonymous. Anonymous vowed to expose the identities of the rapists online. Anonymous confirmed the identities of two of the four alleged rapists.

In the group's statement, it claims to have seen what it calls a confession from one of the young men who allegedly admitted he raped Parsons and named three other boys who had gang raped her as well though the police only brought charges against two of the boys responsible of taking the photo and this circulating it.

| ITEM | NOTES |
|---|---|
| Case name: | Rehtaeh Parsons rape case—Anonymous's attempt to identify the rapists via hacktivism |
| Citation: | No reported case found online—most likely due to the offenders being minors when committing the crime. Case information retrieved from news articles |
| Jurisdiction: | Nova Scotia, Canada |
| Main URL: | *Huffington Post*, "Anonymous Claims Suspect Confessed To Rehtaeh Parsons' Rape," April 12, 2013, available at http://www.huffingtonpost.com/2013/04/12/anonymous-suspect-confession-rehtaeh-parsons-rape_n_3070615.html.<br><br>D. Bates, "Anonymous threaten to unmask boys who 'drove 17-year-old girl to hang herself after they gang raped her and put photo on web'," *Daily Mail*, April 11, 2013, available at http://www.dailymail.co.uk/news/article-2307266/Rehtaeh-Parsons-gang-rape-Anonymous-threaten-unmask-boys-drove-girl-hang-herself.html. |
| Charged with: | In 2014 and 2015, police reopened the case and laid child-pornography-related charges against two teenage males, one eighteen and the other nineteen, for taking and sharing indecent images of a child.<br><br>The identities of the accused are shielded by Canada's Youth Criminal Justice Act because they were under the age of eighteen at the time of the alleged offences. |
| Legislative provisions: | Following the death of Rehtaeh Parsons, Canada passed a Cyber-Safety Act, an anti-cyberbulling law. |
| Main target: | Rehtaeh Parsons's rapists |
| Motivation: | To expose the identities of four rapists after what Anonymous viewed as police inactivity in relation to the case |
| Convicted of: | Members of Anonymous were not convicted in relation to this case |

| | |
|---|---|
| Sentence: | Members of Anonymous were not sentenced in relation to this case.<br><br>The two teenage males who were charged in relation to child-pornography charges were sentenced to probation. One of the charged received a conditional discharge (conviction will not show on his criminal record unless he violates probation). The other male's conviction will be removed from his criminal record after five years. |
| Additional important information: | "Once Anonymous made their rage and intent clear, they were flooded with witness testimony, and from there built the case of the RCMP's incompetence on three points: that dozens of teens and adults had heard the rapists brag about taking part in the gang rape, that the photo taken of the rape was reportedly so widely circulated it's unlikely the authorities ever bothered to try and find it so they might look at the EXIF data, and that Parsons' school did nothing, despite the fact that child pornography was going viral in their hallways." (Waugh, "Rehtaeh Parsons Rape Case Solved by Anonymous.")<br><br>In August 2013, Nova Scotia enacted a law allowing victims of cyberbullying to seek protection, including help in identifying anonymous perpetrators, and to sue the individuals or the parents in the case of minors. The law was passed in response to Parsons's suicide. However, the law was struck down to be redrafted after it was found to violate the Canadian Charter of Rights and Freedoms. |

## ISRAEL

### *State of Israel v Anat Kamm*

The defendant secretly copied thousands of classified (many confidential) military files during her military service, which she leaked, giving the files to a *Haaretz* journalist.

| ITEM | NOTES |
|---|---|
| Case name: | *State of Israel v Anat Kamm* (2010).<br>*Anat Kamm v State of Israel* [2012] |
| Citation: | Case 17959-01-10 |
| Jurisdiction: | Israel, District Court of Tel Aviv Jaffa<br>Israel Supreme Court |

| | |
|---|---|
| Main URL: | Wikipedia, *Anat Kamm-Uri Blau Affair* (October 20, 2018) http://en.wikipedia.org/wiki/Anat_Kamm-Uri_Blau_affair<br><br>Case, http://www.maannews.net/eng/ViewDetails.aspx?ID=275114 |
| Charged with: | Aggravated espionage with intent to harm the security of the state (Penal Law (1977) cl 13b)<br>Leaking secret information with the intention to harm the security of the state (cl 113c) |
| Legislative provisions: | Penal Law (1977) cl 13b and 113c |
| Main target: | Israel Defence Forces (IDF) |
| Motivation: | Kamm wanted to release some details of the IDF's operational procedures in the West Bank as she felt that they should be in the public domain. There was information in the leak that suggested that the military went against a ruling made by an Israeli court against the assassination of wanted militants who could have otherwise been arrested safely. |
| Convicted of: | Leaking classified materials |
| Sentence: | February 6, 2011: Kamm pled guilty in a plea bargain to leaking more than 2,000 secret military documents.<br><br>October 30, 2011: Sentenced to four-and-a-half years' imprisonment (down from a maximum of fifteen years) and eighteen months' probation.<br><br>December 31, 2012: The Supreme Court granted her appeal and shortened her sentence to three-and-a-half years in a majority decision, noting her cooperation in the investigation. |
| Additional important information: | Kamm was released in January 2014 after serving over two years in prison. |

## INDONESIA

### *Wildan Yani Ashari*

Internet café worker Wildan Yani Ashari was arrested by police after he replaced the home page of then-Indonesian President Susilo Bambang Yudhoyono with the message: "This is a PayBack From Jember Hacker Team." This was believed to be in protest at growing corruption and wealth inequality in the country.

| ITEM | NOTES |
|---|---|
| Case name: | Unable to retrieve case. Case facts taken from news articles |
| Citation: | Unknown—unable to retrieve case |
| Jurisdiction: | Indonesia |
| Main URL: | J. Goldman, "Indonesian Government Sites Hacked Following Hacker's Arrest," *eSecurity Planet*, January 31, 2013, available at http://www.esecurityplanet.com/hackers/indonesian-government-sites-hacked-following-hackers-arrest.html |
| Charged with: | Charged under the Information and Electronic Transaction Law (2008) |
| Legislative provisions: | Information and Electronic Transaction Law (2008) |
| Main target: | Indonesian president's website homepage |
| Motivation: | Increased anger over the current administration |
| Convicted of: | Unknown due to not being able to retrieve case. Presumably, sentencing would have been under the Information and Electronic Transaction Law. |
| Sentence: | Facing a maximum sentence of twelve years' imprisonment and a maximum fine of IDR 12 billion (US$1.2 million) |
| Additional important information: | Goldman referenced the *Jakarta Globe*, which reported: "In what were reportedly acts of solidarity for Wildan, Anonymous hackers hacked at least seven sites, including those of the Justice and Human Rights Ministry, the Social Affairs Ministry, the Tourism and Creative Economy Ministry, the Central Statistics Agency (BPS), the Business Competition Supervisory Commission (KPPU) and the Indonesian Embassy in Taskhent."<br><br>Goldman referenced Voice of America's Kate Lamb, who reported: "Instead of the official pages, web users were greeted by a cloaked figure alongside the catchphrase: 'No Army Can Stop an Idea.'"<br><br>Indonesia's then communications minister, Tifatul Sembiring, said there were 36.6 million incidents of hacking against the government in 2012. |

## JAPAN

### *Yusuke Katayama*

Japanese police on Sunday arrested a man, Yusuke Katayama (aka "Demon Killer"), suspected of being behind a computer-hacking campaign following an exhaustive hunt that at one stage had authorities tracking down a cat for clues, according to reports.

| ITEM | NOTES |
|---|---|
| Case name: | Unable to retrieve case. Case facts taken from news articles. |
| Citation: | Unknown—unable to retrieve case |
| Jurisdiction: | Japan, Tokyo District Court |
| Main URL: | *Sydney Morning Herald*, "Man Arrested Over Bizarre Hacking Campaign Involving Cat," February 11, 2013, available at http://www.smh.com.au/technology/technology-news/man-arrested-over-bizarre-hacking-campaign-involving-cat-20130211-2e77o.html |
| Charged with: | He was accused of five charges, including intimidation, business obstruction, using a remote computer, sending a mass-killing threat, and framing innocent people |
| Legislative provisions: | Unknown—unable to retrieve case and details regarding legislative provisions |
| Main target: | Several events around Japan |
| Motivation: | Grudge against authorities |
| Convicted of: | Unknown—unable to retrieve case and details regarding legislative provisions |
| Sentence: | Eight years' imprisonment |
| Additional important information: | According to the *Sydney Morning Herald*, Katayama created a set of riddles and messages going out to media outlets and investigators. He claimed that the details of a computer virus used to dispatch the threats were strapped to a cat living on an island near Tokyo.<br><br>After authorities solved a set of riddles, they found the cat that led to the arrest of Katayama in February 2013. There was a digital memory card around the cat's collar saying "a past experience in a criminal case" had caused the hacker to act. |

## SINGAPORE

### *James Raj Arokiasamy AKA "The Messiah"*

Anonymous member James Raj Arokiasamy (aka "The Messiah") hacked into the official Ang Mo Kio town council website to, he claimed, highlight the website's vulnerability. He also hacked into at least seven organizations' websites.

| ITEM | NOTES |
|---|---|
| Case name: | *James Raj Arokiasamy v Public Prosecutor* |
| Citation: | [2014] 2 SLR 307 ("James Raj") |
| Jurisdiction: | Singapore, States Courts |
| Main URL: | Banyan, "Messiah complicated," *Economist*, December 7, 2013, available at http://www.economist.com/blogs/banyan/2013/12/hacking-singapore.<br><br>Banyan, "Two steps back," *Economist*, February 25, 2014, available at http://www.economist.com/blogs/banyan/2013/06/regulating-singapores-internet.<br><br>I. Poh, "Hacker who called himself 'The Messiah' jailed 4 years and 8 months," *Straits Times*, January 30, 2015, available at https://www.straitstimes.com/singapore/courts-crime/hacker-who-called-himself-the-messiah-jailed-4-years-and-8-months. |
| Charged with: | November 12, 2013: Charged under the Computer Misuse and Cybersecurity Act with carrying out unauthorized modifications to websites |
| Legislative provisions: | Computer Misuse and Cybersecurity Act Ch 50A (Rev Ed 2007) |
| Main target: | Various government, organization, and church websites |
| Motivation: | Retaliation against Singapore's new "Internet-licensing" regime |
| Convicted of: | Pled guilty in January 2015 to thirty-nine computer misuse offences and one count of drug consumption |
| Sentence: | Sentenced to four years and eight months in jail |
| Additional important information: | Denied bail—previously jumped bail and fled to Malaysia after facing drug-consumption charges in 2011.<br><br>Organizations affected by the hack spent about $1.36 million assessing, repairing, and restoring affected computer systems. |

| | |
|---|---|
| | Expecting physical protests, instead the Singaporean government faced a plethora of hacks in protesting the licensing policy after the arrest of Arokiasamy, including the defacement of thirteen school websites on November 22, 2013. |

## GERMANY

### *Andreas-Thomas Vogel*

Andreas-Thomas Vogel launched a denial-of-service attack against the website of German airline Lufthansa in protest of the company's treatment of asylum seekers. Vogel was angered with Lufthansa for making profit from deporting illegal immigrants and he wanted to publicize these grievances. He planned a denial-of-service attack June 20, 2001, and programmed a software, which protesters could download to enable a large number of page views. Vogel posted a call to action on the website libertad.de.

| ITEM | NOTES |
|---|---|
| Case name: | *Libertad.de* (2006) |
| Citation: | File reference 1 Ss 319/05, March 22, 2006 |
| Jurisdiction: | Germany, Higher Regional Court, Frankfurt am Main |
| Main URL: | J. Libbenga, "German court to examine Lufthansa attack," *The Register*, April 1, 2005, available at https://www.theregister.co.uk/2005/04/01/lufthansa_ddos_attack/.<br><br>R. Bendrath, "Frankfurt Appellate Court Says Online Demonstration is Not Coercion," EDRi, June 7, 2006, available at https://edri.org/edrigramnumber4-11demonstration/. |
| Charged with: | Coercion and incitement of alteration of data |
| Legislative provisions: | German Criminal Code sections 240 (coercion), 111 (public incitement to crime), and 303a (data tampering) |
| Main target: | Lufthansa |
| Motivation: | To protest Lufthansa's stance on asylum seekers and achieve publicity |
| Convicted of: | Vogel was indicted and convicted of coercion in the Frankfurt court. The Frankfurt Appellate Court reversed the decision, stating that the DDoS attack was a legitimate exercise of free speech. |

| | |
|---|---|
| Sentence: | Initially, Vogel was sentenced to pay a financial penalty or serve ninety days in jail. However, in his appeal, he was acquitted by the Higher Regional Court of Frankfurt. |
| Additional important information: | The demonstration had 13,614 participants with different IP addresses and encompassed 1,126,200 page views. The damages were about €5,500 for personal costs and €42,000 for further impairments. |

## Note

1. *United States of America v. Ford.*

Page left blank intentionally