Jeremy Hammond on Aaron Swartz and the Criminalization of Digital Dissent

The tragic death of internet freedom fighter Aaron Swartz reveals the government's flawed "cyber security strategy" as well as its systematic corruption involving computer crime investigations, intellectual property law, and government/corporate transparency. In a society supposedly based on principles of democracy and due process, Aaron's efforts to liberate the internet, including free distribution of JSTOR academic essays, access to public court records on PACER, stopping the passage of SOPA/PIPA, and developing the Creative Commons, make him a hero, not a criminal. It is not the "crimes" Aaron may have committed that made him a target of federal prosecution, but his ideas – elaborated in his "Guerrilla Open Access Manifesto" – that the government has found so dangerous. The United States Attorney's aggressive prosecution, riddled with abuse and misconduct, is what led to the death of this hero. This sad and angering chapter should serve as a wake up call for all of us to acknowledge the danger inherent in our criminal justice system.

Aaron's case is part of the recent aggressive, politically-motivated expansion of computer crime law where hackers and activists are increasingly criminalized because of alleged "cyber-terrorist" threats. The United States Attorney for the Southern District of New York, Preet Bharara, whose office is prosecuting me and my co-defendants in the Lulzsec indictment, has used alarmist rhetoric such as the threat of an imminent "Pearl Harbor like cyber attack" to justify these prosecutions. At the same time the government routinely trains and deploys their own hackers to launch sophisticated cyber attacks against the infrastructure of foreign countries, such as the Stuxnet and Flame viruses, without public knowledge, oversight, declarations of war, or consent from international authorities.

DARPA, US Cyber Command, the NSA, and numerous federally-contracted private corporations openly recruit hackers to develop defensive and offensive capabilities and build Orwellian digital surveillance networks, designed not to enhance national security but to advance U.S. imperialism. They even attend and speak at hacker conferences, such as DEFCON, offer to bribe hackerspaces for their research, and created the insulting "National Civic Hacker Day" – efforts which should be boycotted or confronted every step of the way.

Aaron is a hero because he refused to play along with the government's agenda instead he used his brilliance and passion to create a more transparent society. Through the free software movement, open publishing and file sharing, and development of cryptography and anonymity technology, digital activists have revealed the poverty of neo-liberalism and intellectual property. Aaron opposed reducing everything to a commodity to be bought or sold for a profit.

The rise in effectiveness of, and public support for, movements like Anonymous and Wikileaks has led to an expansion of computer crime investigations – most importantly enhancements to 18 U.S.C § 1030, the Computer Fraud and Abuse Act (CFAA). Over the years the CFAA has been amended five times and has gone through a number of important court rulings that have greatly expanded what the act covers concerning "accessing a protected computer without authorization." It is now difficult to determine exactly what conduct would be considered legal. The definition of a "protected computer" has been incrementally expanded to include any government or corporate computer in or outside the U.S. "Authorization," not explicitly defined by the CFAA, has also been expanded to be so ambiguous that any use of a website, network, or PC that is outside of the interest, agenda, or contractual obligations of a private or government entity could be criminalized. In Aaron's case and others the government has defined violating a service's Acceptable Use Policy (*AUP*), Terms of Service (*TOS*), or E*nd-User License Agreement (EULA*) as illegal. Every time you sign up for a service like Gmail, Hotmail, or Facebook and click the "I agree" button that

follows a long contract that no one ever reads, you could be prosecuted under the CFAA if you violate any of the terms.

The sheer number of everyday computer users who could be considered criminals under these broad and ambiguous definitions enables the politically motivated prosecution of anyone who voices dissent. The CFAA should be found unconstitutional under the void-for-vagueness doctrine of the due process clause. Instead, Congress proposed bills last year which would double the statutory maximum sentences and introduce mandatory minimum sentences, similar to the excessive sentences imposed in drug cases which have been widely opposed by many federal and state judges.

The “Operation Payback” case in San Jose, California is another miscarriage of justice where 16 suspected Anonymous members (including a 16 year old boy) allegedly participated in a denial-of-service action against PayPal in protest of it's financial blockade of Wikileaks. Denial-of-service does not “exceed authorized access,” as it is virtually indistinguishable from standard web requests. It is more akin to an electronic sit-in protest, overloading the website's servers making it incapable of serving legitimate traffic, than a criminal act involving stolen private information or destruction of servers. PayPal's website was only slow or unavailable for a matter of hours, yet these digital activists face prison time of more than 10 years, $250,000 in fines, and felony convictions because the government wants to criminalize this form of internet protest and send a warning to would be Wikileaks supporters.

Another recent case is that of Andrew “Weev” Auernheimer, who last November was convicted under the CFAA. Andrew discovered that AT&T was publishing customer names and email addresses on it's public-facing website, without password protection, encryption, or firewalls. Instead of acknowledging their own mistake in violating customer privacy, AT&T sought prison time for Andrew. Andrew has defended his actions saying, “We have not only a right as Americans to analyze things that corporations publish and make publicly accessible but perhaps a moral obligation to tell people about it.”

I am currently facing multiple computer hacking conspiracy charges due to my alleged involvement with Anonymous, LulzSec, andAntiSec, groups which have targeted and exposed corruption in government institutions and corporations such as Stratfor, The Arizona Department of Public Safety, and HB Gary Federal. My potential sentence is dramatically increased because the Patriot Act expanded the CFAA's definition of “loss.” This allowed Stratfor to claim over 5 million dollars in damages, including the exorbitant cost of hiring outside credit protection agencies and “infosec” corporations, purchasing new servers, 1.6 million dollars in “lost potential revenue” for the time their website was down, and even the cost of a 1.3 million dollar settlement for a class action lawsuit filed against them. Coupled with use of “sophisticated means” and “affecting critical infrastructure” sentence enhancements, if convicted at trial I am facing a sentence of 30-years-to-life.

Dirty trial tactics and lengthy sentences are not anomalies but are part of a fundamentally flawed and corrupt two-tiered system of “justice” which seeks to reap profits from the mass incarceration of millions, especially people of color and the impoverished. The use of informants who cooperate in exchange for lighter sentences is not just utilized in the repressive prosecutions of protest movements and manufactured “terrorist” Islamophobic witch-hunts, but also in most drug cases, where defendants face some of the harshest sentences in the world.

For Aaron Swartz, himself facing 13 felony CFAA charges, it is likely that it was this intense pressure from relentless and uncompromising prosecutors, who, while being aware of Aaron's psychological fragility, continued to demand prison time, that led to his untimely death.

Due to widespread public outrage, there is talk of congressional investigations into the CFAA. But since the same Congress had proposed increased penalties not even one year ago, any efforts at reform are unlikely to be more than symbolic. What is needed is not reform but total transformation; not amendments but abolition. Aaron is a hero to me because he did not wait for those in power to realize his vision and change their game, he sought to change the game himself, and he did so without fear of being labeled a criminal and imprisoned

by a backwards system of justice.

We the people demand free and equal access to information and technology. We demand transparency and accountability from governments and big corporations, and privacy for the masses from invasive surveillance networks.

The government will never be forgiven. Aaron Swartz will never be forgotten.

Source

freehammond.com

Pour écrire à Jeremy:

Jeremy Hammond 18729-424
Metropolitan Correctional Center
150 Park Row
New York, New York, 10007