Hacking Authority
Aaron Swartz Memorial Hackathon
Internet Archive, November 8, 2013

Thank you Lisa Rein for organizing this program tonight and thank you to all the people, including Noah Swartz, who have organized these hackathons in memory of Aaron in over 20 locations around the world, from Kathmandu and Bengaluru to the Media Lab and New York and our own national treasure, Noisebridge here in San Francisco.

I want to talk briefly about toxic data, about when hacking might take more than a weekend.

I've had a pretty simplistic job for over 20 years. I copy public data from one location to another. Perhaps the data is transformed, maybe from a scan to an HTML file. Usually I add a few access methods like ftp and rsync to the data for bulk downloads.

But, at the end of the day, all I really do is cp -r.

This job should be simple.

Unfortunately, this data can be very dangerous and you can get burnt. The example I want to use tonight is the project I've been working on for the last few years—publishing the law—but there are many other examples.

We know that ignorance of the law is no excuse. We know that since the days of the Magna Carta that the rule of law means access to justice cannot be sold, denied or delayed. We know that access to the law must be available to all regardless of means, that due process must be observed, that equal protection is a fundamental tenet of our government.

If we are, as John Adams said, ‘‘an empire of laws not of men,’’ we must all know the rules that we as a society have chosen to govern ourselves with.

A few years ago, I started publishing a special kind of law, public safety codes. An example is the National Electrical Code, which is required by the federal government and all 50 states. If you violate the National Electrical Code, you can go to jail. This law is there to protect our homes and offices, to make our society safer.

Over the last few years, I have copied over 28,000 such technical public safety codes from all over the world.

There is an obvious question anybody might ask, which is why would this be a big deal? Freedom of speech and rule of law mean that I should be able to read the law and I should be able to speak the law. But, in our modern society, public safety codes that are required by law have been locked away.

Until we started working in this area, none of these codes were available on the Internet. You could only get them by purchasing them from the code developers, who have asserted copyright. The codes are incorporated into law, but the code people say that they need to charge you money because that is what sustains their work.

They say if people copy the law willy-nilly, they will loose control over their assets and go broke. They say anarchy will ensue if anybody can speak the law without a license.

This argument is—of course—a bit nuts. The code people are all nonprofits or, in many countries, an arm of the government. They make money in a huge number of ways—this is a multibillion dollar industry.

Developers of the National Electrical Code have received the gold standard of approval from government and they can and do leverage that enviable market position to sell certification, handbooks, training, annotated codes, and all sorts of valuable and expensive services.

I'm fine with these folks charging for training and handbooks, but we the people own the law, not judges or legislators and certainly not the code people.

In August, 3 of these standards bodies sued us in federal court. The law suit lists 10 lawyers from 3 fancy law firms working on the case for the plaintiffs.

The president of the American National Standards Institute has launched a huge PR campaign, the code people have made this their number one public policy issue.

This is a big deal. If I were to pirate a movie and post it, statutory damages for such a violation is $150,000. Now, I've done nothing wrong, I'm not a pirate, I haven't violated copyright, but think about $150,000 statutory damages for each of 28,000 documents and you realize the $4.2 billion potential downside to this activity. This data is dangerous.

What the code people have released, just last week, is an alternative to my site. Their new so-called "law reading room" requires you to preregister, you have to install a PDF DRM plugin on your computer, they will monitor your usage, and you will be able to see the standard—but not print, copy, save, or even take a screen dump.

They will report on your usage of the law to various international organizations and use your name to up-sell you on various products to pay for the $1 million salaries these nonprofits all bestow on their CEOs.

There are many things that are perfect for hackathons, and I'm amazed at the number of topics that have sprung up on the wiki for this weekend. But, before you hit cp -r on data, it is worth stopping and thinking for a bit, and asking yourself if you are prepared to see that copy through.

One of the things that Aaron did very well was work over the long term on issues, and I think when you deal with toxic data it is important to take that long view.

I've been reading a lot about how people confront authority, and I wanted to share a few of the lessons I've absorbed.

First, if there is something wrong with our society—and there is certainly very much wrong with our society—change often occurs by confronting specific geeky issues and seeing them through.

Rosa Parks just wanted to sit on a bus seat. James Meredith applied to attend the University of Mississippi. Mohandas Gandhi choose to object to the requirement that colored citizens of the British empire visiting South Africa required a registration stamp, but the whites did not.

Those specific issues are proxies for broader social change, but focusing on a specific issue forces authority to the table. Gandhi said that "the removal of a step from a staircase brings down the whole of it."

When you look at the work of Thurgood Marshall in the United States and Gandhi in South Africa, you see that these were not isolated hacks that they performed, in each case there was a very long-term strategy. These issues are not solved overnight, they require years, sometimes decades.

If you are to confront authority, then you must do so carefully and deliberately. When I started publishing standards, I made copies of them and sent them to the code people with a letter requesting their comment.

When we get a takedown letter from authorities from around the world, they get back a carefully considered explanation of the basis for the action and we respectfully and explicitly decline to comply with their demands. We make clear that this is a matter of conscience, not one of conspiracy or profit.

There is one more lesson, which is that while we must convince authority to change their ways—merely liberating data is not enough, you must get them to encourage the activity—we must also convince ourselves.

Change comes from movements, when many people begin working towards a common aim. When we question authority, we do so to put them on notice, but also to educate ourselves. If we all stand together, we can tell the authorities "you can govern us, but only so long as we remain the governed." That is the basis of civil disobedience. That takes time and patience.

If you wish to question authority and hack our society for the better, you must work systematically and deliberately. We win when authority chooses to change, when we convince them of the truth and justice and moral right of the questions we have asked. We win when we stand together. Think carefully before you copy.