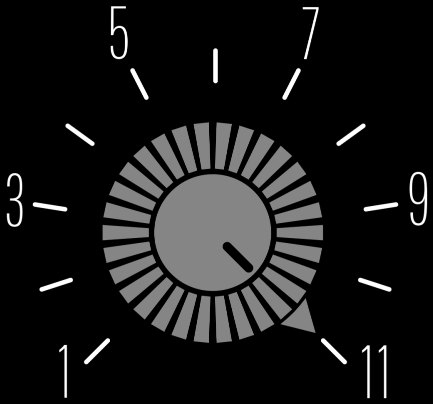
THE ELEVENTH HOPE

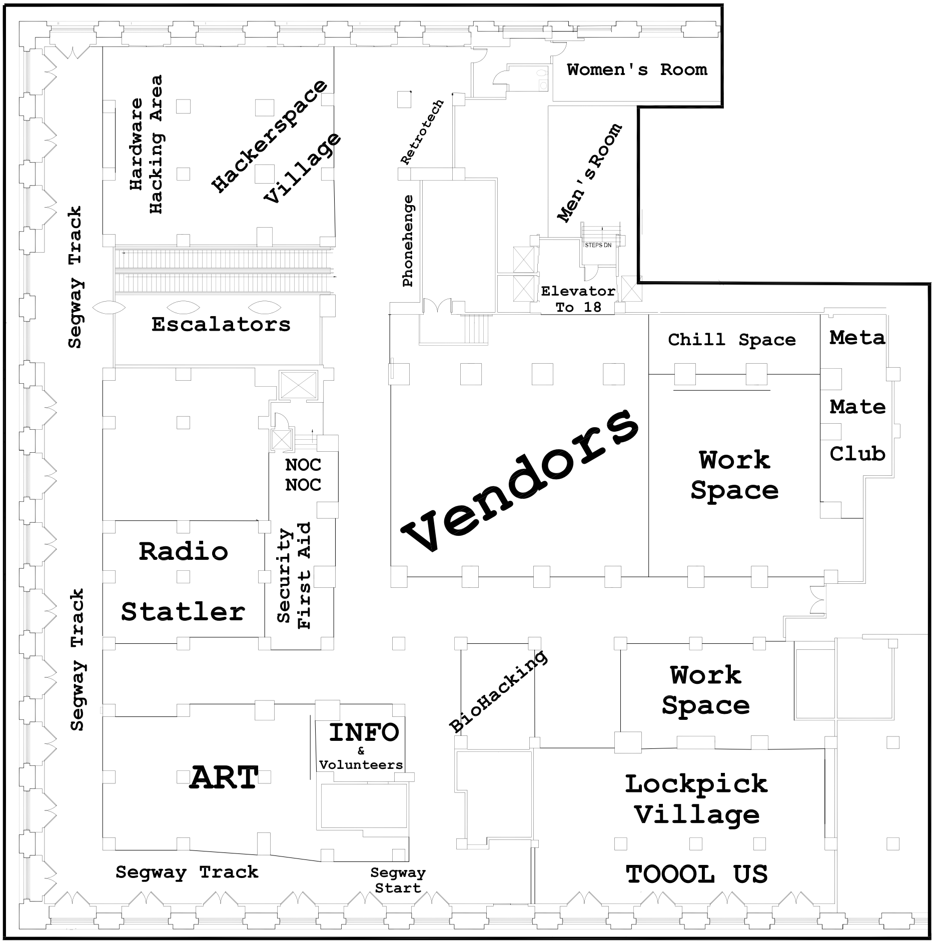
TAKING IT TO ELEVEN



JULY 22nd-24th, 2016
HOTEL PENNSYLVANIA, NEW YORK CITY

xi.hope.net
@hopeconf

SECOND FLOOR



Flip to the inside back cover
for eighteenth floor information

THE ELEVENTH HOPE

Welcome to The Eleventh HOPE! It's hard to believe that this is the eleventh time we've had a Hackers On Planet Earth conference, but then there's so much in the hacker community that's equally difficult to believe.

This year in particular we feel as if what we have here is a little bastion of sanity in an otherwise crazy world. We find ourselves sandwiched right in between the two biggest shit-shows on the planet: the Republican and the Democratic national conventions. So it may be a bit competitive for several thousand hackers to grab all the headlines this weekend. But we all know this is where the real stories are being written and where the future of technology is sprouting.

If you're coming from Cleveland, relax - it's finally over and you're now amongst friends. If you're heading on to Philadelphia, let us help you create fond memories this weekend that will get you through the utter hell you'll experience there.

The Eleventh HOPE is all about excess. We've taken the dial and turned it up a notch to eleven. That means that everything is just a little bit louder, a little bit stronger, a little more relevant. Many of us have been working eleven-hour days for the past eleven months. Eleven is at the heart of it all. Did you know there were eleven time zones in the Soviet Union? Eleven. That's how big they were.

But we digress. You're at the hacker event of the year and you have an All Access Pass! (Well, most of you do, anyway.) And with that access, you will each have a truly unique experience as you pick and choose what talks and activities to participate in. We have so many this year.

As you enter, take a good look at all that's going on in the Mezzanine. We've got representation from hackers all over the globe in so many different areas. There's the Hackerspace Village which has displays and demos from hackerspaces of all sorts, a Hardware Hacking area where you can learn all sorts of skills, the Lockpick Village where you can test and improve your skills on opening locks, a biohacking section which could easily replicate and take over the entire space, Segway rides, a wide assortment of vendors, Club-Mate *and* Meta Mate, hacker art, our own radio station (Radio Statler), an impressive "retrotech" display, and, of course, Phonehenge, which needs no explanation and shall receive none.

Your journey will continue on an express elevator which bypasses the entire hotel and brings you all the way to the 18th floor where our four speaker tracks will be ongoing throughout the weekend. Many people make this their home for all of HOPE, but this is hardly necessary since our ten gigabit Internet connection (which we've turned up to eleven for that extra kick) ensures that all talks will be streamed to wherever you happen to be. So please don't plant roots in a single room. Move around freely and accept that you won't be able to experience *everything* in this brief time period. Just know that what you do experience will be pretty damn cool and memorable. We also have expanded workshop space on the 6th floor, as well as a room for extended discussions after selected 18th floor talks. Just take the elevator down to the 6th floor! It's that simple. At night we'll be having concerts on the first floor, midnight movies and some new interactive stuff going on in the speaker rooms. Remember: sleep can wait.

Take some time to read over the wide variety of talks we're presenting this year and then take a look at the stories of the people who are presenting them. We think you'll be blown away by the talent and diversity that's currently under this roof. We're damn proud of where this community has journeyed and we look forward to seeing it evolve even more. At HOPE we take great pride in mixing college professors, teenagers, corporate executives, spies, and activists into our speaking schedule where they are all received as equals. We hope you listen to them - and speak when inspired.

Remember also that you're right smack in the middle of New York City and that all sorts of amazing things are happening constantly. The city is friendly and always open, but it can be overwhelming for a first-timer. So if you want to explore, go with friends but don't stay away from HOPE for too long - the city will always be there, after all.

Please be kind to our many volunteers who provide everything from A/V setup to security to answering the many questions of our attendees. This conference simply wouldn't be possible without them. If you want to help, just stop by the InfoDesk on the Mezzanine.

Please also be good to the hotel, as this is our home for the weekend and they have been really good to *us* over the years. The amount of history this place has seen throughout the past century is simply mind-boggling. We hope to make a little more of that history here at The Eleventh HOPE. Enjoy!

TALKS

2016 Car Hacking Tools
Craig Smith, Eric Evenchick
This presentation will focus on some of the most recent car hacker tools and techniques. You will learn how to quickly get set up to do car hacks, both professionally and in your garage. After the demos, Craig and Eric will open up for a full-on Ask Me Anything (AMA) style panel discussion where you are free to ask any car hacking related questions you feel like.
Friday 1600 Noether

Accessibility:
A Creative Challenge to Living without Sight
Shaf Patel
In this presentation, Shaf will be discussing the various methods blind and visually impaired people use to accomplish everyday tasks, with an emphasis on technology, screen reading software, and application design from a blind person's perspective. There will be live demos of screen reading software, OCR apps for smartphones, wearable devices, and mobility aids (time permitting). There will also be a discussion on myths and stigmas relating to blindness, an audience Q&A regarding accommodating those with a visual impairment, and tips and tricks for those who develop applications to include accessibility in their core design.
Friday 1700 Friedman

All Ages: How to Build a Movement
Deb Nicholson, Molly de Blanc
We want the free software movement to keep growing and one facet of successful movement building is embracing a multi-generational community. The good news is that there is no age requirement for using, promoting, and contributing to free software. The bad news is that we aren't always doing a great job of facilitating a diverse, inter-generational movement. We'll take a look at what we're currently doing to bring in young people, how we are treating older people in our communities, and where there is room for improvement.
Saturday 1800 Noether

Anti-Forensics AF
int0x80 (of Dual Core)
This presentation is the screaming goat anti-forensics version of those "Stupid Pet Tricks" segments on late night U.S. talk shows. Nothing groundbreaking here, but we'll cover new and trolly techniques that forensic investigators haven't considered or encountered. Intended targets cover a variety of OS platforms.
Sunday 1300 Noether

Ask the EFF: The Year in Digital Civil Liberties
Kurt Opsahl, Jacob Hoffman-Andrews,
Vivian Brown, Parker Higgins
Get the latest information about how the law is racing to catch up with technological change from staffers at the Electronic Frontier Foundation, the nation's premiere digital civil liberties group fighting for freedom and privacy in the computer age. This session will include updates on current EFF issues such as surveillance online, encryption (and backdoors), and fighting efforts to use intellectual property claims to shut down free speech and halt innovation. The panel will also include a discussion on their technology project to protect privacy and speech online, updates on cases and legislation affecting security research, and much more. Half the session will be given over to question-and-answer, so it's your chance to ask EFF questions about the law and technology issues that are important to you.
Friday 1500 Lamarr

Attacking the Source:
Surreptitious Software Features
(and How to Become Extremely Paranoid)
Joshua
Forget about network perimeters - an organization's real attack surface is made up of which codebases can be interacted with or altered. This talk explores the past history and the methods available for maliciously altering codebases and it even includes how an attacker can bring their code into your organization without even touching your perimeter. Topics covered include everything from conceptualizing an attack path to the execution of it; including obtaining relevant target information, exploiting the human element, writing plausibly deniable vulnerable source code, and backdooring binaries.
Saturday 2300 Friedman

Biology for Hackers and Hacking for Biology
Kevin Chen, Jameson Dungan
Biotechnology is information technology - software that you can code and engineer. It is becoming very clear that biology needs to be approached with the same hacker ethic and mentality as software and hardware. Furthermore, the technology needed to hack biology is becoming much more accessible. In this panel, you'll learn some of the basics of biology using terms and analogies that would be useful for hackers and for people in information technology. Basic points will be outlined on how to get started in biohacking, both virtually and physically. This talk will also cover the current state of biotechnology and how biology can be approached and improved upon through the philosophy and culture of hacking.
Friday 1000 Lamarr

The Black Holes in Our Surveillance Map

Marcy Wheeler

While Edward Snowden has revealed a lot about the NSA's surveillance, our federal and local governments conduct a great deal of surveillance we still don't know about. We can begin to identify what that surveillance is by identifying the empty spaces - in criminal cases, in legislation, or timelines - where such surveillance must be. This talk will attempt to point to some of the black holes in our surveillance map, both ones we know exist and the places where one must exist. That's the first step in working collaboratively to expose that surveillance. More importantly, this talk will focus on how to see these black holes, and how people around the country can work together to make them visible again.

Sunday 1600 Lamarr

Bringing Down the Great Cryptowall

Weston Hecker

Ransomware has been running rampant for the past six years and there has been very little done to stop infections aside from deprecated signature scans and classic malware scanners. This talk will unveil some proof of concepts that work on even the most current versions of the ransomware plaguing the networks of today, from a hacked USB device to a form of backup to making your physical machine look like a virtual machine which the malware ignores.

Sunday 1800 Lamarr

Bring the Noise: Ten Years of Obfuscation as Counter-Surveillance

Daniel C. Howe

It has been a decade now since the release of TrackMeNot, the first privacy tool to leverage obfuscation for counter-surveillance. In the interim, obfuscation has been actively developed, with new tools exploring its use for email (ScareMail), location-tracking (CacheCloak), advertising (AdNauseam), DNA analysis (Invisible), and beyond. This talk reviews the development of the strategy and considers some of the questions it raises for the tool-making community. Daniel will debut AdNauseam 2.0, the first cross-platform production release of AdNauseam, which aims at nothing less than ending advertising-based surveillance as we know it. Obfuscation can be defined as the strategy of using noise to hide one's true interests and/or confuse an adversary. As obfuscation is relatively flexible in its use, it holds unique promise as a strategy for DIY privacy and security. TrackMeNot was the first privacy tool to leverage obfuscation online, protecting web searchers from search engine profiling by hiding their queries in a cloud of generated noise. AdNauseam directs similar techniques at the advertising networks that track users across the web, polluting user profiles and subverting the economic system that drives this pervasive form of surveillance.

Saturday 1600 Friedman

Building Your Own Tor-centric ISP for Fun and (non)Profit

Gareth Llewellyn

Following the Snowden revelations and with the U.K. government's revival of the Snooper's Charter legislation, Gareth was one of many people who accepted the EFF Tor challenge. Unfortunately, many U.K. ISPs' colocation providers do not appreciate Tor exits and, after several abruptly terminated servers, he decided to build his own privacy centric, non-profit ISP so he could operate Tor exits and offer Unix shells, etc. on his own terms. This talk explores the process of becoming a local Internet registry in Europe, dealing with RIR polices such as IPv4 exhaustion, Tor abuse complaints, and the deployment of a broadband product that only has a Tor bridge instead of a next hop at the end of a DSL connection.

Saturday 1500 Friedman

Can We Sue Ourselves Secure? The Legal System's Role in Protecting Us in the Era of Mass Data Leaks and Internet of Things

Alex Muentz

Large data breach stories just merge into one another. Weak IoT security is no secret. Yet the marketplace isn't fixing this problem. Can the legal system play a part? This talk will discuss current approaches under U.S. regulatory, product liability, and tort law to encourage vendors to secure their devices and services.

Sunday 1400 Lamarr

CAPTCHAs - Building and Breaking

dr_dave, r3dfish

CAPTCHAs are the most common form of web activity security and they play an important role in regulating online activity. CAPTCHAs keep bots and "blackhats" from abusing online resources by proving a user's humanity via solving a challenge that consists of a hard AI problem. CAPTCHA development is a constantly evolving arms race with new styles and designs being created by site administrators and broken by attackers every day. In order to keep the world wide web usable, site administrators must constantly work on developing new methods and improving CAPTCHAs to prevent automated abuse.

This talk will cover the basics of what CAPTCHAs are, what type of security they provide, the major types of CAPTCHAs, and how to attack them. The speakers will also discuss criteria used when designing their CAPTCHA framework and cover some academic literature that is relevant to the field. They will look at popular tools and services currently used to attack CAPTCHAs and provide some insight into the current state of bot identification.

A fresh new CAPTCHA design will be presented that uses human emotion recognition as the "hard AI" challenge. Speakers will demonstrate how they have achieved their desired usability, scalability, and robustness levels via a real world implementation. An overview of the tools and tool chain used (MS Emotion API, GIMP, Google APIs, Python, Django) to create the CAPTCHA challenges will be detailed. The session will conclude with a user study and provide an analysis of the results with a discussion about some of the limitations of the project.

Saturday 2300 Noether

Censorship- and Coercion-Resistant Network Architectures

Ed Platt

Decentralized network architectures can protect against vulnerabilities not addressed by strong encryption. Encryption works well, but only when private keys can be kept secret and ciphertext can get to its destination intact. Encrypted messages can be surveilled by acquiring private keys (FBI and Lavabit/Apple), man-in-the-middle attacks (NSA QUANTUM), or censored by blocking communication entirely (Pakistan and YouTube). These attacks are difficult to protect against because they are social rather than technological. But they all have one thing in common: they require centralization. Censorship and man-in-the-middle attacks target communication bottlenecks and legal coercion targets a small number of legal entities. This talk will discuss decentralized approaches to attack tolerance, including ongoing original research.

Sunday 1300 Friedman

Censorship, Social Media, and the Presidential Election

Elissa Shevinsky

There is increasing interest in the ability of companies like Facebook and Twitter to influence elections. What are the roles and responsibilities of these companies to be fair and impartial? Newspapers express bias and endorse candidates. Facebook employees have even asked if they have a responsibility to (try to) prevent Donald Trump from becoming elected. Twitter has been accused of censoring tweets supporting Donald Trump, while also allegedly censoring posts that were unfavorable to Hillary Clinton. While that is certainly legal, is it acceptable to us as citizens? If not, what can we do about it? And what makes our expectations of bias from Twitter different from our expectations of *The New York Times* or *The Daily News?*

This talk is an exploration of the ways that social media can influence elections, and what that means for us as citizens.

Friday 1700 Noether

Chinese Mechanical Locks - Insight into a Hidden World of Locks

Lucas Zhao (UrbanHawk)

Chinese-made locks have traditionally had poor reputations. The Chinese-made locks that we usually encounter in our day-to-day lives always seem to be low quality, cheap, and insecure at best, so it may seem that this is all that the Chinese make. However, there is a whole other world of lock designs that are sold exclusively to the Chinese domestic market. In this presentation, a variety of different Chinese lock designs will be discussed, from the prominent and innovative, such as the Yuema free spinning cylinder line of locks to the relatively obscure, such as the Chinese take on the Corbin Emhart rotating pin design. This talk will cover the defeats of these locks, both theoretical and practical, in addition to the steps Chinese lock companies have taken to address these vulnerabilities, as well as the reasons behind the constant innovation.

Friday 1500 Friedman

Closing Ceremonies

We've finally gotten a bill before Congress designating the Monday after HOPE as a day when one doesn't have to go to work or school. Many employers already recognize as fruitless any expectation that work will get done on that day. So don't feel bad about staying late on Sunday in order to attend our final session of the conference - the infamous HOPE closing ceremonies. This is where we go over what went right and what went wrong this weekend - and where we let you know what we had to go through in order to pull this whole thing off. And, if we're not totally fed up and disgusted, there may be talk of a sequel.

Sunday 1900 Lamarr

The Code Archive

Filippo Valsorda, Salman Aljammaz

Archiving web pages is hard. Crawling, images, assets... Javascript! But archiving code is not. It comes as content-addressed objects neatly packaged in repositories and tagged with refs. It compresses well. Changes can be detected in real time with the GitHub Firehose API.

Nevertheless, we need to do it today while the host is healthy, and not wait for it to start bundling adware or slowly fade away. Otherwise, in ten years we'll find ourselves running unreproducible binaries on Javascript emulators, or unable to build the software that could recover all our pictures because that one dependency is missing.

This is a talk about building The Code Archive, a Wayback Machine for git. Every time a repository changes on GitHub, Code Archive systems fetch it and archive all the files, commits, tags, and branches as they were at that time. Then you can clone a repository as it was at any point in time, even if the original has been rebased, has disappeared, or GitHub is down. There's a lot of fun to be had when (ab)using the git protocol to clone and pull millions of repositories to the same database. Speakers will show what git looks like on the wire and how fetches are optimized. Also, all the Go code powering the Archive is available... on GitHub.

Friday 1800 Noether

Code Is from Mars, the Courts Are from Venus: Reverse Engineering Legal Developments on Reverse Engineering

Sebastian Holst, Alexander Urbelis

This past May, in response to the growing sophistication of cyberattacks and application exploits, U.S. lawmakers (almost unanimously) passed the first-ever federal law concerning trade

secret protection: the Defense of Trade Secrets Act. Under the DTSA, however, reverse engineering is protected and deemed 100 percent legal. Within weeks, the EU followed with their own directive increasing trade secret protection while protecting reverse engineering. This talk discusses how this new law impacts reverse engineering, the pros and cons of tying reverse engineering to the courts, best practices for code development, limitations on reverse engineering, counterattacks to those limitations, and counterattacks to the counterattacks.
Saturday 2200 Noether

Coding by Voice with Open Source Speech Recognition

David Williams-King
Carpal tunnel and repetitive strain injuries can prevent programmers from typing for months at a time. Fortunately, it is possible to replace the keyboard with speech recognition - David writes Linux systems code by voice. The key is to develop a voice grammar customized for programming. A community has evolved around hacking the commercial Dragon NaturallySpeaking to use custom grammars, but this method suffers from fragmentation, a steep learning curve, and frustrating installation difficulties. In an attempt to make voice coding more accessible, David created a new speech recognition system called Silvius, built on open-source software with free speech models. It can run on cloud servers for ease of setup, or locally for the best latency. He and his collaborators have also prototyped a hardware dongle which types Silvius keystrokes using a fake USB keyboard, and requires no software installation. This talk will include live voice-coding demos with both Dragon and Silvius. The hope is that Silvius will lower the bar for experimentation and innovation, and encourage ordinary programmers to try voice coding, instead of waiting until a crippling injury throws them in at the deep end.
Friday 2000 Friedman

Come into My (Biohacking) Lab and See What's on the Slab

Tom Keenan
It's 1979 and bright young hackers are torturing their Commodore PETs and Apple IIs to make all the pagers beep on a university campus, or take control of a dam in Alberta. (Both are true stories - Tom was there.)

Fast forward to 2019 and their children (or grandchildren) are doing the same thing - driven by our universal desire to make technology "do things it's not supposed to be able to do." Except now, the role of personal computers is being played by CRISPR Cas9 gene editing gear that they bought for a few dollars on eBay. What can they do with it? Make animals glow in the dark? Destroy all life on this planet? Hold us hostage with bio-ransomware?

This talk will examine the fast moving science behind biohacking and how it will change our lives. It will also apply the "technocreep framework" to predict which aspects of biohacking will be considered cool and which will seem creepy, even to the freethinking folks who attend HOPE. As a bonus, you'll learn what happens when you put sponges and electrodes on your head and run direct current through your brain.
Sunday 1600 Noether

Computer Science Curricula's Failure - What Can We Do Now?

Ming Chow, Roy Wattanasin
We are still facing the same security vulnerabilities from over a decade ago. The problems are not going away anytime soon and a reason is because computer science curricula are still churning out students who are not even exposed to security. This talk will address the lack of emphasis on information security in computer science curricula, how CS curricula have an obligation, how to gradually fix the problem by integrating security into many computer science undergraduate and graduate classes, and success stories from students. This talk will also discuss what Tufts and Brandeis are currently working on to further address the security education problem by creating a joint cyber security and policy program that spans multiple departments. Additional points and feedback from the audience are encouraged to help with the issue.
Saturday 1800 Friedman

Constructing Exocortices with Huginn and Halo

The Doctor
Huginn (https://github.com/cantino/huginn) is an open-source human capability-amplifying and augmentation system which implements scenarios - networks of autonomous software agents that collectively analyze data and use it to accomplish sophisticated tasks on behalf of its users. External to Huginn is the Halo (https://github.com/virtadpt/exocortex-halo), a collection of software constructs optimized for carrying out tasks too complex for Huginn due to resource requirements, contention, or reliance upon lower level libraries, including synthesizing speech, placing Voice over IP calls, and carrying out limited secretarial duties to facilitate human interaction. The development histories of both Huginn and Halo will be discussed during the first part of the talk with representative examples of the presenter's agent networks to demonstrate the architecture of scenarios as well as solutions to practical problems. Agents, the basic building blocks of Huginn scenarios and the software constructs of Halo will be briefly detailed to give an overview of some of possibilities of the two interrelated software systems. The talk will conclude with brief descriptions of some of the tasks that HOPE attendees can accomplish through the use of both Huginn and Halo.
Sunday 1400 Noether

Crypto War II: Updates from the Trenches

Matt Blaze, Sandy Clark
For several years, law enforcement has been complaining that legal wiretaps are "going dark" (especially when encryption is used), and has been

lobbying lawmakers to mandate "surveillance-friendly" technology that allows the government to break encryption and unlock devices under certain circumstances. At the same time, computer and network security is universally recognized to be in an increasingly dangerous state of peril, and technologists worry that "backdoor" mandates will only make things worse.

We've been here before, not long ago. In the 1990s, after the government proposed the "Clipper Chip" key escrow system, we had a similar debate with similar stakes. It was finally resolved when the government essentially gave up and finally allowed cryptography to proliferate.

This talk will review the current cryptography debate, will examine the risks of the "keys under doormats" that the FBI is asking for, and will explore technical alternatives that could satisfy the needs of law enforcement without making computer security more of a mess than it already is. In particular, Matt and Sandy will examine the viability, and risks, of law enforcement exploitation of existing vulnerabilities in targets' devices to obtain wiretap evidence.

Friday 1700 Lamarr

De-Anonymizing Bitcoin One Transaction at a Time

David Décary-Hétu, Mathieu Lavoie

Bitcoin is an established virtual currency well known for enabling affordable and efficient transfers of money between individuals and entities. With its market cap of over $7 billion and hundreds of thousands per day, the Bitcoin currency has become popular enough for offenders to be able to hide among its users when they purchase illicit goods and services online or need to receive extortion payments. The aims of this presentation are twofold. The first is to present an open-source tool developed by the panelists that analyzes all of the Bitcoin transactions and regroups Bitcoin addresses based on their incoming and outgoing transactions. This allows for a more accurate mapping of individuals' online activities no matter how many Bitcoin addresses they are using. The tool, as well as a database of all nodes identified by the tool, will be released on the day of the conference. The second aim of this presentation is to provide real world use cases for the tool to better understand online illicit activities. To do so, David and Mathieu will present two case studies that will follow the evolution through time of the revenues generated by online illicit groups and the strategies they used to manage the incoming bitcoins. This talk will be of interest to attendees looking to better understand how the Bitcoin currency works and the attacks that can be used to de-anonymize Bitcoin users. A live demonstration will explain how the open-source tool works and the strategies that could be used to preserve one's anonymity in the Bitcoin network.

Friday 1400 Noether

Deconstructing Ad Networks for Fun and Profit

Timothy Libert

This talk focuses on an open-source software tool, webXray, which detects the presence of third-party data flows on the web and attributes such flows to the corporations which receive user data. The talk will first describe the challenges, dead ends, and solutions encountered in developing the software so that developers and novices in the audience may understand the nature of the problem domain. Second, the talk will cover how to use the tool to analyze targeted populations of web pages with an emphasis on scaling and cost considerations. Third, the talk will describe findings in three areas: tracking found on medical websites, Chinese websites, and newspaper websites including measures of user exposure to malware-hosting domains embedded in ostensibly trusted websites. The talk will conclude with a theoretical discussion of how those seeking to leverage ad networks to deliver malware may pick the best networks suited to their objectives.

Sunday 1700 Friedman

Democratizing Wireless Networks with LimeSDR: Open Source, Field-Programmable RF Technology

Ebrahim Bushehri

This talk presents new, low-cost, open-source, field programmable RF technology, where flexibility is extended from the digital to the RF domain. See demonstrations from the open-source community using the LimeSDR platform, which incorporates two transmitters and two receivers covering 100kHz to 3.8GHz which can emulate GSM, LTE, UMTS, Wi-Fi, Bluetooth, Zigbee, RFID, HDTV, radio astronomy, passive RADAR, 2G/3G/4G cellsites, IoT gateway, amateur radio, wireless keyboard/mouse transmission/detection, aviation transponders, utility meters, satellite reception, remote tire pressure monitoring, drone command and control, RF test and measurement, and more.

Sunday 1600 Friedman

Detour Through Their Minds: How Everyday People Think the Internet Works

Gillian "Gus" Andrews

When you work in IT or Infosec, it may feel like you're constantly fighting a battle to bring the non-technical people you work with up to speed on how technologies work. When you help family members with their computer problems, you may just want to throw up your hands and scream "It's no use! They just don't get it!" But when you dig a little deeper, as a number of studies have done, you find that the average person does have some knowledge about how the Internet works. They build on this knowledge every day - but sometimes they're incorporating what they've learned from that scene on *NCIS* where two people are using a keyboard at once. They may hold some common misconceptions. Or they may be sooo close and just need one little additional piece of information.

Gus will share insights from the study she has been working on for the past year about average people's

mental models of the Internet, along with a number of other studies from human-computer interaction and security research. Key concepts like "mental models," "fragile knowledge," "stereotype threat," and "learned helplessness" will be explored. In addition, ways the gaps in people's knowledge impact digital security and how we might strategize on a large scale to help fill those gaps will be explored. You'll come away with better strategies for helping empower the non-technical folks in your life to solve their own problems.
Saturday 1700 Noether

FOIA and Public Records Hacking: How to Complete a FOIA Request or Dox Yourself via the Privacy Act

Caitlin Kelly Henry

Learn how the key to writing successful FOIA requests is reverse engineering agency data structures. This talk will include an overview on writing successful FOIA or Privacy Act requests, including updates from recent cases. You will learn the step by step process of drafting a request, using the FBI as an example. This talk is great for activists, students, researchers, journalists, and people with security clearances (especially after the OPM hack).
Sunday 1100 Friedman

FOIA at Fifty

Jameel Jaffer, David Pozen

The Supreme Court has stated that the Freedom of Information Act "defines a structural necessity in a real democracy." On the 50th anniversary of its enactment, now is an opportune moment to reflect on the role FOIA has played in our legal and political system. This conversation will bring together Jameel Jaffer from the ACLU and David Pozen from Columbia Law School to consider the past, present, and future of FOIA. They will discuss virtues and drawbacks of the FOIA model, FOIA's relationship with technology and other transparency mechanisms, the effectiveness (or ineffectiveness) of FOIA in the national security context in particular, and lessons to learn from foreign and state-level approaches to regulating government openness.
Saturday 1500 Lamarr

Freedom and Privacy in Our Lives, Our Governments, and Our Schools

Richard Stallman

If we don't control the program, it controls us. It is clearer every year that nonfree programs, beyond the basic injustice of giving the developer or owner unjust power over the users, also tends to be malware, for instance designed to restrict users or snoop on them. Since government agencies and schools require people to run software to exercise their rights, this software must all be free, but increasingly they impose use of nonfree software and commercial snooping services. We must now organize to demand that they stop.
Sunday 1200 Lamarr (2 Hours)

F*ck it, We'll Do It Live: Eight Years of Radio Statler!

Beaches, Nikgod, TechDarko, Bunni3burn, Johnny Xmas, Stoppay

Since 2008, Radio Statler has been broadcasting original content from HOPE to the rest of the world: interviews with speakers, extended Q&As, panels, and the occasional glimpse into everything that happens outside the talk rooms. The panel will take you through how and why Radio Statler! started, the obstacles faced running a temporary radio studio, and some of the war stories of the things that have gone terribly, terribly wrong along the way.
Friday 2300 Lamarr

Go Hack Yourself!

Michael Hernandez

Hacking of all kinds requires discipline and concentration. Over the past few years, Michael has been seriously practicing yoga and meditation and has found that it's been a great help in many areas of his life, including his work as a hacker and programmer. Eating healthy and exercising your mind and body sounds like a load of crap to a lot of hackers but the reality is that if you want to have a long sustained life that you can continue to use for hacking and exploration, you'll want to keep your mind and body healthy. Practicing concentration daily and learning to meditate can help you literally hack your mind, and help you make changes within yourself you might have thought impossible. Practicing discipline in these areas will also bring confidence and inner strength that will help you in whatever kind of hacking you're doing or planning to do.
Sunday 1000 Friedman

Hackers Are Whistleblowers Too: Practical Solidarity with the Courage Foundation

Nathan Fuller, Grace North, Naomi Colvin, Carey Shenkman, Lauri Love, Yan Zhu

In the two years since the Courage Foundation was launched, they have supported beneficiaries at every stage of the information exposure process: hacktivists, investigative journalists, and human rights defenders. Most recently, the Courage Foundation announced their campaign to raise European funds and awareness for Chelsea Manning. They believe the blurred line between activists and journalists needs to be embraced as a spectrum of solidarity; each of these actors needs the others to bring information to public attention, and so each deserve our support.

While whistleblowers like Edward Snowden enjoy international appreciation, hackers are often marginalized as outsiders who don't enact real change. But it's high time we recognized their value, understanding that - since the information war occurs largely online - digital activists are those that governments seek to make the biggest examples of.

In this session, the speakers will provide updates on their ongoing cases, including Barrett Brown's and Chelsea Manning's, discuss some of the systemic issues encountered along the way, and then solicit your input. This is a two-way conversation. The purpose is to bring the kind of support Edward Snowden gets to all beneficiaries - and your ideas of how to get there are welcomed at this panel discussion.

Naomi Colvin and Nathan Fuller from the Courage Foundation will recap what we've learned in the past two years and what they plan to do going forward. Grace North, prison-rights activist heading the Jeremy Hammond support network, who has also worked closely with Lauri Love on his case, will discuss the challenges Jeremy continues to face and what we need to do for Lauri to prevent him finding himself in the same situation. Lauri will be joining the discussion by video feed to talk about his ongoing battle against extradition to the United States. Yan Zhu, security software engineer and friend of Chelsea Manning, will talk about how we can help Chelsea from the outside. Carey Shenkman, First Amendment and human rights attorney with the Center for Constitutional Rights representing journalists including Julian Assange and WikiLeaks, will explain the need for a public interest defense for journalistic sources.

Sunday 1000 Noether

Hacking DNA: Heritage and Health Care

Janine Medina

Humans are the compilation of bio-code that has been changing and evolving for almost 200,000 years. In some ways, we are the oldest open-source project around, but not on GitHub - yet. In years past, DNA sequencing and analysis was available only to a handful of scientists with huge labs and nearly unlimited budgets. Now that world is changing. There are products and services available today that bring individual DNA sequencing to your fingertips, and digging into your own source code has never been easier or cheaper. Analyzing DNA can not only reveal secret ancestries, but can provide a level of insight and history into your health that doctors in the past have only dreamed of. This talk will discuss how and why you can perform your own genetic background check, and what it means for your past, present, and future.

Saturday 2000 Friedman

Hacking Housing

Luke Iseman, Heather Stewart

Luke and Heather will discuss their work building shipping container based, off-grid, open-source houses and factories. They will provide a crash course in getting and converting containers, including specific recommendations on how to modify them into solar-powered, comfortable living and working spaces. This is relevant because it's silly for us to live and work in corporate-owned environments built by somebody else, rather than hacking our own sustainable, affordable alternatives.

Sunday 1500 Friedman

Hacking Machine Learning Algorithms

Kyle Polich

Algorithms control more and more of the systems we interact with on a daily basis. Critical decisions are executing without direct oversight by machine learning models. These systems, like any system, should be continuously taken apart and inspected to see how they work. Examining a machine learning model is not as easy as examining source code. This talk goes into detail on how to hack machine learning models and similar systems. Could an algorithm be racist? How can we detect it? Live examples in Python will be demoed and available on GitHub, and only basic programming knowledge is required to understand the talk and reproduce the examples.

Friday 2200 Lamarr

Hacking Sex: Toys, Tools, and Tips for Empowerment and Pleasure

Kit Stubbs

Hacker culture celebrates technological empowerment: encouraging people to move beyond passive consumerism towards building and modifying technology to better meet their own needs. Hacking sex means expanding our definition of "sex;" recognizing that no two of us have the exact same biology, (a)sexuality, or desires; and building and modifying toys and equipment to enhance our own pleasure.

Join Kit "where did this b!tch get [their] doctorate" Stubbs for a look at technological empowerment for sexuality and pleasure. Recent developments in sex/tech will be covered, including crowdfunded sex toys, a patent troll, open-source sex toys, and 3D printing, with plenty of resources for folks new to sex/kink-positive DIY.

Saturday 1900 Noether

Hacking through Business: Theory and Logistics

Mitch Altman, Limor Fried, Phil Torrone,
Ben Dubin-Thaler
Moderators: Sean Auriti (Theory),
Charles Beckwith (Logistics)

It's rare that you see an engineer as CEO, but occasionally taking a technical idea to its logical conclusion requires the person who knows what's going on inside the black box to take the reigns. Someone who knew everything they needed to know to start the project technologically is suddenly confronted with human problems and legal issues and paths forward that might require new types of specialized knowledge and very different gut decisions. This extended panel discussion will address both the blue sky possibilities of a company led by tech, as well as the plethora of challenges thrown at anyone who finds it necessary to not let someone else run their business.

Sunday 1700 Noether (2 hours)

How Anonymous Narrowly Evaded Being Framed as Cyberterrorists

Gabriella "Biella" Coleman

Over the years, Biella has used many different words and phrases to describe Anonymous: hydra, trickster, confusing, enchanting, controversial, frustrating, unpredictable, stupid, and *really* stupid. But rarely has she ever argued seriously against the idea that Anonymous is tantamount to cyberterrorism. How did Anonymous avoid the title of cyberterrorists when they were perfectly positioned to earn it? Biella will discuss the reasons such as the adoption of the Guy Fawkes mask, the timing of their most important operations, and the role of pop cultural representations of hackers like *Mr. Robot* that allowed them to narrowly escape this designation.

Friday 1300 Lamarr

How to Start a Crypto Party

Comet Crowbar

Learning about encryption tools can be intimidating. If you don't feel comfortable with a computer, or are deathly afraid of some long-winded mansplaining of how something works, it's probably a nightmare or doesn't feel worth doing at all. And who cares about combating NSA surveillance when you get frustrated/annoyed at "all this computer stuff?" Enter the Crypto Party: a nonhierarchical space to get together and ask questions, learn from each other, and ideally to leave the event with encryption and anonymity tools set up on your computer. It's a space to eat snacks, get answers, and, if no one knows, you can figure it out together. There are solutions to resist surveillance, but it is still a problem of accessibility to get the solutions to the people in a way they can understand. And there are already enough borders in this world! In this talk, Comet Crowbar will share her experience with organizing monthly crypto parties in the Boston area. Having been "crypto-ized" while living in Berlin, she was inspired by the do-it-yourself crypto parties she encountered there, and has aspired to bring the idea back to occupied Turtle Island. And so far, so good. Comet will also show examples of her zines and artwork that she uses as a medium to bring political issues to the mainstream by creating culture. Become the media! And start a crypto party in your hometown. This talk is for everyone and will be using accessible language.

Friday 1800 Friedman

How to Torrent a Pharmaceutical Drug

Michael Swan Laufer, Bethany (Benny) Koval

Why are people still being left to die from treatable diseases when they can't afford the arbitrarily inflated prices of patent-protected medications? As hackers, we believe that when the infrastructure fails, we must have a way to fall back to DIY methods. Medicine should not be an exception to this. Pharmaceuticals are just chemicals, chemicals are made using chemistry, and chemistry can be automated. Come learn how anyone can make patent-protected medications at home using a new open-source automated chemical reaction chamber made from off-the-shelf parts. One no longer has to have a science background to do chemistry. We can save our own lives. Speakers will detail how the mechanism can be built, how it is programmed, and distribute the plans and programs live at the talk. The programs for drug synthesis and the design of the mechanism can be shared over any digital channel - and can be improved and modified by any end user. A highly controversial drug will be synthesized live on stage during the talk.

Friday 1100 Friedman

I "Hacked" for China

Zimmer Barnes

For six months, Zimmer was hacker-in-residence for a top Chinese engineering university, tasked with mentoring students and building projects. He encountered brilliant Chinese hackers and incredible startups and built several projects aimed at reducing air pollution in Beijing. After his residency, he stayed in Beijing for four months and helped to cofound Q Space, Beijing's first feminist makerspace which now holds regular workshops and events, and has over 300 members in their group chat. If you've ever wanted to travel to China as a hacker, Zimmer will be happy to share everything he wishes he knew before he went.

Friday 1100 Lamarr

Information Overload and the "Last Foot" Problem

Nick Lum, Andrew Cantino

There's so much to read and so little time. Unlike past generations who awoke to find a single newspaper on their doorstep, we open our smartphones and computers to find thousands of newspapers, websites, and blogs beckoning our attention. With this deluge of reading material, we're left with a "last foot" problem: how do we get all this information from our screens into our brains? This talk will give a brief history of the written word, describe neurological aspects of the reading process, and explore some of the new innovations that aim to let us read more quickly and efficiently on-screen.

Saturday 2200 Friedman

Iridium Satellite Hacking

Stefan "Sec" Zehl, schneider

The Iridium satellite system has been in orbit for over 15 years now and provides various data and voice services. This talk will show how to use Software Defined Radio (SDR) to receive and decode data from the Iridium satellite network and how a lot of reverse engineering was performed to understand the protocol and decode the details.

Sunday 1200 Noether

Is the Brain the Next Hackable Driver?

Ellen Pearlman

Do our EEG, fMRI, and other biometric data contain the essence of who we are and what we think? In the future, could this data be used as an identifier for security and thought modification as well as exploring virtual worlds? If our "brainotypes" or "brain fingerprints" and concurrent cognitive processes are monitored, how do we prepare for this looming horizon? Though no one is entirely sure, these questions invite both scientific and metaphorical approaches addressing these issues. Ellen will discuss the emergence of technologies,

research, and methods on brain datatyping; privacy and its ethical implications; sending and receiving motor commands between two different brains; moving robotic prosthesis through thoughts; the formation of memory; manipulating memory via frequencies of light; and hacking brain computer interfaces (BCIs) to extract vital information. Keeping these methods and techniques in mind, she will also show a brief excerpt from her own creation "Noor - a Brain Opera" which asks the question "Is there a place in human consciousness where surveillance cannot go?"
Friday 1400 Friedman

Keynote Address - Cory Doctorow

We are so stoked to have Cory Doctorow as our keynote this year. We've been trying to get the stars to align for many HOPEs, and this time they did. But we're glad we waited until now, since so much has happened in the past few years that Cory has been on top of - Snowden, Manning, privacy, copyright issues, surveillance - and his talk will no doubt open your eyes even more. As co-editor of *Boing Boing,* special advisor to the Electronic Frontier Foundation, a prolific writer of both fiction and non-fiction, and a vocal proponent of changing our copyright laws, Cory really has a lot of super-important and relevant thoughts to share with our HOPE audience.
Saturday 1300 Lamarr, Noether, Friedman

Leak Hypocrisy: A Conversation on Whistleblowers, Sources, and the Label "Espionage"

Jesselyn Radack, Carey Shenkman, Naomi Colvin

The two-tiered injustice system: high-level officials who leak for political gain get cover; those blowing the whistle on crimes and abuse face decades in prison. The problem is urgent, costing daily the liberty of Edward Snowden, Chelsea Manning, and many whistleblowers, as well as the liberty of Julian Assange, a publisher.

In this critical moment, join two leading lawyers and the Courage Foundation for a conversation on attacks on freedom of expression, the failure of internal oversight mechanisms, the serious need for a "public interest" defense for truth tellers, and the promise of a growing international movement to promote and protect them.
Saturday 1100 Lamarr

LinkNYC Spy Stations

Deborah Natsios, John Young

The infamous team from cryptome.org and cartome.org will report on the new LinkNYC kiosks' origins, legislation, design, manufacture, installation, and operation, along with the civil liberties threat they pose and options we can implement to inhibit and avoid their spying capabilities.
Sunday 1100 Lamarr

Lockpicking in Real Life versus on the Screen

Nite 0wl, Max Power, Deviant Ollam, and many others from TOOOL and Locksport International

We all know that Hollywood has a difficult time portraying hackers accurately. This quirk often extends to the realm of showing lockpicking in movies and on TV. But sometimes, a film gets it really right! This talk is both an introduction to lockpicking (in case you still need to learn) as well as a walk through some of the best - and some of the worst - scenes of lockpicking that have ever been seen by movie and TV audiences.

Learn about how to be a better lockpicker and a better filmmaker... all at the same time!
Saturday 1600 Lamarr

LockSport Roadshow: Bring Your Oddities!

TOOOL and friends

There have been plenty of talks at HOPE teaching you to pick conventional locks. But what about *non*-conventional locks?

This panel - which will require much audience participation - is all about unique and interesting locks. Have a weird lock or even a strange key and want to know more about it? Bring it to the stage! If you can stump our esteemed panel, you'll win a prize!

Don't be shy... bring out your unique and strange lock hardware and, if you're really brave, give the panel a chance to try to pick it!
Friday 1900 Lamarr

Matehacking: Legalizing Autonomous Production and Permaculture - Establishing a Hack Farm

Fabrício do Canto

This talk will focus on a proposal to create a "mate hacking farm." Technologization is running full power in the direction of monoculture and industrial mass scale drying of mate using eucalyptus burning as an energy source. This will bring dramatic ethnological and environmental impact to the South American Pampas.

Hackers can play an important role by developing easy to construct, recycled, upcycled, and DIY technology for the decentralized production of yerba mate in both traditional and new ways. This draws attention to the need for a solution for food sovereignty in the southern hemisphere.

The "mate hacking farm" would be a fantastic place to tunnel in, get wired, and push new technologies and open-source forest management solutions. Any activistic, fantastical, solidary and commerce-free ideas and concepts are welcome to be executed there and planned for now.
Friday 1200 Friedman

The Mathematical Mesh and the New Cryptography

Phillip Hallam-Baker

Recent events have reminded us again of the urgent need to make encryption ubiquitous on the Internet. Yet, with the exception of Transport Layer Security, encryption remains the domain of "expert" users.

Hope X (2014) was held in the immediate aftermath of the publication of the Snowden papers. In the two years since, there have been many important developments in the standards world (in particular, IEEE, IETF, W3C) that are designed to defeat mass surveillance. These efforts include randomized MAC addresses for Wi-Fi, Certificate Transparency, and DNS privacy.

This talk will review those efforts and provide a preview of the next generation of cryptographic applications currently being built. The PrismProof email system described at Hope X has become the core of the Mathematical Mesh, an infrastructure that solves the encryption usability problem. Once a device is connected to a user's Mesh profile, all the network application settings (including for OpenPGP, SSH, etc.) are managed automatically from an application controlled by the user.

Solving the usability problem and the current move to elliptic curve based cryptography allows Internet security to move beyond the limited cryptographic primitives used in TLS, SSH, and OpenPGP. Public key encryption offers more than just encryption and signatures. Future message encryption schemes will allow end-to-end secure communication within groups of users without the sender having to create decryption material for each intended recipient.

Sunday 1700 Lamarr

Medical Devices: Pwnage and Honeypots

Scott Erven, Adam Brand

We know medical devices are exposed to the Internet both directly and indirectly, so just how hard is it to take it to the next step in an attack and gain remote administrative access to these critical life saving devices? This talk will discuss over 30 CVEs Scott has reported over the last few years that will demonstrate how an attacker can gain remote administrative access to medical devices and supporting systems. Over 100 remote service and support credentials for medical devices will be presented.

So is an attack against medical devices a reality or just a myth? Now that we know these devices have Internet facing exposure and are vulnerable to exploit, are they being targeted? Scott and Adam will discuss six months of medical device honeypot research, showing the implications of these patient care devices increasing their connectivity and steps that can be taken to reduce risk associated with these life saving devices.

Saturday 1500 Noether

Mesh VPN with Service Discovery

Spencer Krum

Tinc provides a secure mesh VPN for any number of hosts. Spencer and his friends used this to build a network linking their homes, laptops, and various hosted machines. They started doing some cool things with it such as UPnP and NFS, things that would be impossible to do securely over the public Internet. This talk will highlight their experiences along the way.

Friday 2100 Friedman

Monitoring Dusty War Zones and Tropical Paradises - Being a Broadcast Anthropologist

Mark Fahey

Tuning in distant foreign radio and television stations is a conduit to unique and exotic information. These signals are often confronting, uncensored, and unsanitized. In the western world, we blur or pixelate images of death and torture, but signals from war zones or rebellions show tragedies happening live on the air. Other signals broadcast the joy of life on this planet through exotic song, music, and film. Digital wide-band recordings of the electromagnetic spectrum allow virtual time travel, a form of mental teleportation whereby recorded spectrum is tuned to hear stations as if they were being tuned in real time. Take a virtual tour of Mark's monitoring station in Sydney, Australia which is wired to access the world's mass media via whatever delivery conduit is needed to capture the content. The station receives hundreds of thousands of inbound digital audio and video channels that let him monitor domestic radio and television from most parts of the world. If he wants to watch breakfast television from Tibet, or maybe the nightly news from the remote Pacific islands of Wallis and Futuna, then it's available in perfect studio quality. You'll also see his visits to remote broadcasters and rare, uncensored video from telejournalists that captures the tragedies and joy served up by our planet.

Saturday 1000 Lamarr

National Security Letters: The Checks and Balances Aren't Strong Enough - Sometimes They're Nonexistent

Nicholas Merrill

Twelve years have passed since Nicholas Merrill first began his lawsuit challenging the constitutionality of the USA PATRIOT Act and, specifically, the warrantless searches known as National Security Letters (NSLs). Now that he can tell the full story, what really happened? How much has actually changed because of the 12-year court case? If the government lost, why are NSLs still being issued at a rate of 50,000 per year? Who is doing anything about this problem, and what are they doing? What are the respective roles of litigation, legislation, and technical approaches to the issue of privacy?

Friday 2200 Noether

The Next Billion Certificates: Let's Encrypt and Scaling the Web PKI

Jacob Hoffman-Andrews

Let's Encrypt is a free and automated certificate authority to encrypt the web, launched in December 2015. Jacob will explain why HTTPS is important to Internet freedom and the role certificate authorities play. He'll give an introduction to the ACME protocol that Let's Encrypt uses to automate validation and issuance, discuss Let's Encrypt's progress by the numbers, and outline some of its future plans.

Sunday 1000 Lamarr

Now and Then, Here and There

Jason Scott

In the last few years, the Internet Archive (archive.org) has steered deeply into the worlds of software history, hacker presentations, and artifacts from all parts of technology's past and present. Jason Scott, the Archive's software curator and inside man, walks through both the current stacks of technology and hacker culture history and reveals in what directions the nonprofit library hopes to expand. Lots of amusing imagery and endless lost weekends will ensue.

Saturday 2200 Lamarr

The Onion Report

asn, John Brooks, Nima Fatemi, David Goulet

The Tor community, network, and ecosystem are growing and evolving at a very fast pace - from new secure applications using Tor to deploying relays in public libraries around the world. Tor as a project, but first and foremost as a large community, is at the forefront of technical, social, economical, political, and cultural battles pertaining to anonymity and basic human rights.

This talk will cover the state of Tor on all levels: organizational, community, and technical. Recent and upcoming software developments, movement in onion (aka hidden) services land, attacks on the network and how we are fighting back, community projects, and much more will be covered.

This is not about the Dark Web but rather about a Secure Web (copyleft pending).

Friday 1600 Lamarr

Only You Can Stop Police Surveillance - Here's How

Matt Cagle, Mariko Hirose, Jared Friend

As America debates policing reforms, police departments continue to rapidly acquire surveillance technology in secret, often with federal grant funds. Whether it's Stingray cell surveillance devices or social media monitoring software, invasive tools are being deployed without democratic debate or safeguards to prevent racial profiling. But while this war against surveillance may seem like a losing one at times, advocates are winning key battles in cities across the U.S. Join civil liberties advocates and ACLU attorneys from New York, San Francisco, and Seattle for a discussion of how to increase transparency, frame the debate, and create meaningful policy reforms that protect civil liberties and civil rights.

Friday 1300 Noether

Open Source Malware Lab

Robert Simmons

The landscape of open-source malware analysis tools improves every day. A malware analysis lab can be thought of as a set of entry points into a tool chain. The main entry points are a file, a URL, a network traffic capture, and a memory image. This talk is an examination of the major open-source tools that satisfy the analysis requirements for each of these entry points. Each tool's output can potentially feed into another tool for further analysis. The linking of one tool to the next in a tool chain allows one to build a comprehensive automated malware analysis lab using open-source software.

Saturday 2100 Noether

Orbital Mechanics Ate My Weblog

Edward K. Beale

At high latitudes, orbital mechanics make deep-ocean Internet almost impossible. In most cases, it is not wattage, atmospheric attenuation, latency, or antenna position that are the culprits - it is geometry. In 2001, Edward blogged about his voyage to Antarctica aboard an icebreaker as lead helicopter pilot. Twelve years later, he completed a full shipboard circumnavigation and delivered a daily weblog to several hundred crowdsourced readers, later self-published in the book *West By Sea.* Across those years, Internet access got better, but at high latitudes it still sucked. In addition to sea stories about massaging crappy packets, this talk outlines the basics of deep ocean bandwidth in layman's terms, gives a short modern history of the tools and tech, outlines new innovations that meld terrestrial and orbital bandwidth for offshore users, and focuses on the burgeoning need for better solutions at high latitudes.

Saturday 1100 Friedman

The Ownerless Library

Paul Kernfeld

Managing a subversive digital library takes courage: Julian Assange is in exile and the founders of The Pirate Bay received prison sentences. How can we design a digital library without a central administrator to attack? To meet this challenge, we'll sneak data into the Bitcoin blockchain, permanently destroy bitcoins, and build a peer-to-peer network entirely out of browsers. If we do it right, we won't be able to take the library down even if we wanted to!

Saturday 1700 Friedman

The Panama Papers and the Law Firm Behind It: Shady Lawyers Caught With Their Pants Down

Alexander Urbelis, Manos Megagiannis

The Panama Papers are beyond question one of the most significant acts of whistleblowing next to the Snowden revelations. Yet, the full measure of what has been leaked remains to be disclosed to the public, raising considerable questions about what happened, who is implicated, and the legal and illegal acts of Mossack Fonseca, the law firm behind the breach. This talk will review what the Panama Papers leak is, introduce the breached law firm, examine Mossack Fonseca's explanation of the breach, deconstruct and debunk their explanation, present MF systems that were more likely the cause of the breach, present alternative and more plausible theories of the breach, examine MF communications that indicate questionable and possibly illegal activity within and without the United States, step through the legal implications of MF's activities, identify the right Infosec questions clients should be asking of law

firms, and provide a question and answer session to ruminate about the breach and its source.
Friday 1400 Lamarr

A Penetration Tester's Guide to the Azure Cloud
Apostolos Mastoris

The wide adoption and the benefits of cloud computing has led many users and enterprises to move their applications and infrastructure towards the Cloud. However, the nature of the Cloud introduces new security challenges, therefore organizations are required to ensure that such hosted deployments do not expose them to additional risk. Auditing cloud services has become an essential task and, in order to carry out such assessments, familiarization with certain components of the target environments is required. This talk will provide insight into the Microsoft Azure Cloud service and present practical advice on performing security assessments on Azure-hosted deployments. More specifically, it will demystify the main components of a cloud service and dive further into Azure-specific features. The main security controls and configurations associated with each of the mainstream Azure components will also be explored. Areas that will be covered include role-based security, secure networking features, perimeter security, encryption capability, auditing, and monitoring of activities within the Azure Cloud environment. Additionally, the talk will include the demonstration of a new tool that uses the Azure PowerShell cmdlets to collect verbose information about the main components within a deployment. The tool also provides functionality to visualize the components within a network infrastructure using an interactive representation of the topology and the associations between the deployment's components.
Friday 2000 Noether

The Phuture of Phreaking
The Cheshire Catalyst

Phone phreaking has always been about the exploration of the PSTN (Public Switched Telephone Network). Richard Cheshire will discuss phreaking in the age of VoIP (Voice over Internet Protocol). Downloading the Phone Loser's blue box app is not a prerequisite.
Friday 1000 Noether

Presidential Twitter Bot Experience
Roni Bandini

Until a few months back, Argentina had a monarchy-styled government that included huge corruption, nepotism, and political violence. Néstor Kirchner was president for four years, then his wife, Cristina Fernández de Kirchner, was president for the following eight years. Instead of giving press conferences, she used the official Twitter account (@CFKArgentina) to spread Goebbels-styled propaganda, send threats to the opposition, and exalt fanatics of all kinds.

This talk will explain the adaptation of an old chatter bot engine designed for a porn web site that now is used for a fake presidential Twitter account. Day by day, lots of political tweets are answered by this bot and almost no one detects that a piece of code is responsible for the mise-en-scène.
Sunday 1200 Friedman

Privacy, Anonymity, and Individuality - The Final Battle Begins
Steven Rambam

First came the assault on privacy. Name, address, telephone, DOB, SSN, physical description, friends, family, likes, dislikes, habits, hobbies, beliefs, religion, sexual orientation, finances, every granular detail of a person's life, all logged, indexed, analyzed and cross-referenced. Then came the gathering of location and communication data. Cell phones, apps, metro cards, license plate readers and toll tags, credit card use, IP addresses and authenticated logins, tower info, router proximity, networked "things" everywhere reporting on activity and location, astoundingly accurate facial recognition mated with analytics and "gigapixel" cameras and, worst of all, mindlessly self-contributed posts, tweets, and "check-ins," all constantly reporting a subject's location 24-7-365, to such a degree of accuracy that "predictive profiling" knows where you will likely be next Thursday afternoon. Today we are experiencing constant efforts to shred anonymity. Forensic linguistics, browser fingerprinting, lifestyle and behavior analysis, metadata of all types, HTML5, IPv6, and daily emerging "advances" in surveillance technologies - some seemingly science fiction but real - are combining to make constant, mobile identification and absolute loss of anonymity inevitable. And, now, predictably, the final efforts to homogenize: the "siloing" and Balkanization of the Internet. As Internet use becomes more and more self-restricted to a few large providers, as users increasingly never leave the single ecosystem of a Facebook or a Google, as the massive firehose of information on the Internet is "curated" and "managed" by persons who believe that they know best what news and opinions you should have available to read, see, and believe, the bias of a few will eventually determine what you believe. What is propaganda? What is truth? You simply won't know. In a tradition dating back to the first HOPE conference, for three full hours Steven Rambam will detail the latest trends in privacy invasion and will demonstrate cutting-edge anonymity-shredding surveillance technologies. Drones will fly, a "privacy victim" will undergo digital proctology, a Q&A period will be provided, and fun will be had by all.
Saturday 1700 Lamarr (3 hours)

Privacy Badger and Panopticlick vs. the Trackers, Round 1
William Budington, Cooper Quintin

Increasingly, as you navigate the web, your movements are being tracked. Even when you reject browser cookies, you transmit unique information that makes your browser personally identifiable. Ad tech and tracking companies are transforming the web into a platform where your user data is brokered and exchanged freely without your consent or even knowledge - and there is a true absence of limits to

the methods trackers are willing to use to get that data from you. Luckily, there is hope. The Electronic Frontier Foundation (EFF) has been developing technologies that let you know exactly how much of this data you are giving out as you browse, as well as releasing tools to help you protect yourselves against the trackers. Panopticlick and Privacy Badger help you keep your personal data private - and this talk will show you how.
Friday 1800 Lamarr

SecureDrop: Two Years on and Beyond

Garrett Robinson
Two years ago, Freedom of the Press Foundation introduced HOPE to their just-launched SecureDrop project, the open-source whistleblower submission system for journalists and news organizations that was originally created by the late Aaron Swartz. Now over three dozen news organizations around the world are using SecureDrop, and they've learned a ton about how journalists and sources interact securely. This talk will share a lot of this information for the first time. How is SecureDrop working in newsrooms? What challenges and threats does the system face? And what does the next generation SecureDrop look like?
Friday 2000 Lamarr

The Securitization of Cyberspace and Its Impact on Human Rights

Sacha van Geffen, Mallory Knodel,
Stefania Milan, Camille Francoise
A handful of representatives from governments, the private sector, and civil society comprise an international working group of the Freedom Online Coalition (called "An Internet Free and Secure") that is tasked with harmonizing human rights and security. But protected rights like privacy and free speech already *are* security. Rights and security are not antithetical; they are compatible. Government power and corporate profits fuel the rights versus security narrative that has dominated the U.S. and Europe since the introduction of the U.S. Patriot Act. To dislodge this dominant narrative, this panel has developed over the course of two years a human rights respecting definition of cyber security and a normative statement of policy recommendations for how cyber security policy should be written and implemented if it is to truly be secure, e.g. to protect human rights.
Sunday 1100 Noether

Security Options for High Risk Travelers

Ryan Lackey
Aggressive surveillance and espionage has long been a fact of life for government agents traveling to hostile nations but, increasingly, economic espionage is waged against visitors who neither have the expectation that they're a target nor the resources to adequately defend themselves from plausible threats. This talk will present tools, techniques, and procedures which will allow non-nation-state international travelers to defend themselves from government, criminal, and commercial monitoring, with a bias toward free and open-source options readily adopted by potential targets.
Friday 2300 Noether

Seven Continents: A Telecom Informer World Tour

TProphet
As The Telecom Informer, TProphet has traveled all over the world and visited all seven continents. Everyone knows that different countries have different cultures, but did you know that there are different *telephone* cultures? The way that people use and interact with telecommunications services is different all over the world. Learn about some of the off-the-beaten-track places he has visited (such as Antarctica, Ecuador, Myanmar, and North Korea) and how, no matter where you live, phones bring the world closer together.
Friday 2100 Noether

Show Networks

John Huntington
Behind the scenes on most any large entertainment production today - from an arena spectacle to a theme park dark ride, from a concert tour to a Broadway stage - you will find Ethernet switches, cat 5 cables, and IP addresses all playing a critical role carrying a variety of control protocols that make these sophisticated shows possible. In this talk, John Huntington, author of *Show Networks and Control Systems,* will give an overview of the ways that networks are used on shows, and why and how we use equipment from traditional IT applications. In addition, applications from real shows will be featured, including a detailed exploration of the sophisticated control network for the Gravesend Inn haunted attraction.
Friday 1300 Friedman

The Silk Road to Life without Parole - A Deeper Look at the Trial of Ross Ulbricht

Joshua Horowitz, Andy Greenberg,
Patrick Howell O'Neill, Alex Winter
Join Joshua Horowitz, one of Ross Ulbricht's defense attorneys, tech journalists Andy Greenberg and Patrick Howell O'Neill, and filmmaker Alex Winter for an in-depth discussion of the Silk Road case. All panelists attended Ulbricht's trial.

Greenberg and O'Neill have written extensively about the now legendary black market's rise and fall and Alex Winter directed the documentary *Deep Web,* with exclusive access to the Ulbricht family and defense team. In this panel discussion, they'll examine the less-discussed aspects of Ulbricht's case, including the role of two corrupt federal agents in the Silk Road investigation, the indictment of Ulbricht's alleged mentor and consigliere Variety Jones, and Ulbricht's controversial life sentence without parole.
Saturday 1600 Noether

Slicing and Dicing Espionage: The Technical Aspect of Hunting Spies

James M. Atkinson
TSCM (Technical Security Countermeasures) is

the U.S. federal government's abbreviation for electronic counter-surveillance. This talk is about the art and science of TSCM and how it's used to actually catch spies in the act. It will include photos and visual aids about how a TSCM professional goes from a mere hunch to tracing the spy right to their listening post. While this presentation will obviously be unclassified, it will focus on facilities used by the U.S. intelligence community and DoD contractors, methods used to "sweep" these targeted locations for electronic surveillance, and how actual "bugs" were found. It will include sufficient technical detail to enable the HOPE audience to apply technical search methods to their own locations and communications equipment.

This will be a distinctly hardware or physical layer oriented presentation, which will assume a limited knowledge by the attendee of the physical aspects of technical espionage. The presentation will cover an actual espionage operation uncovered using these methods, and what was done to exploit the spy who was exploiting the bug, and how they were neutralized. Methods used for frustrating technical spies, including state actors, will be discussed, as well as methods for identifying an informant within a group. The concept of "nexus" will be discussed as it applies to counterespionage and how scientific methods are used to locate a nexus between the target and a pathway, between the pathway and the listening post, and from the listening post to the spy.

This talk is designed to have a broad appeal, and will include details about bug sweeps and spy hunting jobs that the speaker recently led. The audience may become a bit paranoid learning how vulnerable they are to illegal electronic eavesdropping, but methods will be presented on how they can lawfully enhance their privacy. Legal protections that U.S. citizens have against government eavesdropping, and how to frustrate state-sponsored eavesdroppers, will be discussed - as well as how and where to look for bugs and other eavesdropping devices and how to use improvised methods when only low-tech tools are available.

Highlighting this talk will be examples of four specific bug sweeps (two CIA cover operations and two DoD contractor locations) and, while it will not include classified information, the U.S. government will not be amused. Photographs, blueprints, drawings, cable traces, spectrum analyzer screenshots, and related measurements will be shown so the audience can grasp the art and science of effective TSCM.

Friday 2100 Lamarr

Smart Cities and Blockchains: New Techno-Utopian Dreams or Nightmares?

Burcu Baykurt, James Cropcho, Benjamin Dean

History is littered with techno-utopian visions, particularly those of powerful American industrialists. Henry Ford's Fordlandia, Walt Disney's Epcot, Peter Thiel's Seasteading. Technologies play a recurring role in inspiring and enabling these attempts to forge or impose new governmental and/or social relations. Techno-utopian dreams are once again emerging in the form of sensor and data-driven "smart" cities and decentralized, blockchain-based organizations. What are the similarities and differences between techno-utopian visions over time? What role does technology play in forming and operationalizing these visions? Who ultimately defines what a perfect society is? How does this determine whether the techno-utopian visions end up as dreams or nightmares?

Friday 1900 Noether

Social Engineering

Emmanuel Goldstein and friends

Since 1994, we've had a lot of fun with this panel, where we not only share stories of some of our most memorable social engineering adventures of years past, but we try and create some new memories live on stage over a good old-fashioned telephone line. For those not familiar, social engineering is the art of getting information out of people, information that you usually have absolutely no business possessing. The ability to gain a stranger's trust, knowing what to ask for, and (perhaps most importantly) how to deal with failing miserably are all vital skills in the pursuit of unauthorized information. This panel is open to suggestion on targets to try, as well as open to new panelists who want to share their stories and skills. Leave your info at the information desk. (Be sure to include your Social Security number and mother's maiden name.)

Saturday 2100 Lamarr, Friedman

Spy Hard with a Vengeance: How One City Stood up to the Department of Homeland Security

aestetix, Brian Hofer

This talk will cover the reign of surveillance that has secretly taken over the United States at the local level through use of federal grant money, and offer suggestions on how we can fight back. It's the story of how the Department of Homeland Security (DHS) tried to create a fusion center in Oakland, California. In particular, the presentation will share details of the Oakland privacy policy the speakers helped create in response to this intrusive spy system, and the advocacy that led to its creation. The hope is to teach the framework that was created, shed light on how these issues affect both Americans and Europeans, and show how businesses and governments can find a balance between security and privacy.

Sunday 1500 Noether

Stealing Bitcoin with Math

Filippo Valsorda, Ryan Castellucci

Bitcoin is the best thing that ever happened to bored applied cryptographers: it's a public database of keys and signatures made by quickly developed software that, when broken, drops money as if it was loot.

This talk will look at mistakes old and new that enabled attacks: from ECDSA repeated nonces to using Math.random to make keys, from double spending and transaction malleability to crappy brainwallets.

The bad news is that most vulnerable wallets were emptied a long time ago. The good news is that we get to look at how (and how fast) "cryptocriminals" operate in the process. In any case, new tools that implement some of the attacks will be demoed and released.

No need to be a Bitcoin or crypto wizard - everything you need in order to understand what those poor victims didn't will be explained.

Saturday 2000 Lamarr

Sunset or Evolution of the PSTN?

Fred Goldstein

The public switched telephone network has seen better days. With interest diverted to the Internet and mobile services, the venerable PSTN that we know and love seems like it's ready for the knackers. But maybe that's not quite right. True, the dominant carriers have let their wireline networks rot, and the TDM technology that seemed so advanced two decades ago is this year's black-and-white TV set. But the PSTN has undergone many rounds of evolution, from cord switchboards to Strowger dial to common control to analog ESS to digital. Now SIP signaling and IP networks are taking over. It's the big carriers who want to claim that this is no longer the PSTN so that they can get out of their regulatory obligations and exercise their remaining monopoly muscle. And the folks in Washington who are supposed to be supervising this still haven't figured out what VoIP is, so no wonder it's all such a mess. Let's see where the PSTN is going and what that means to us.

Sunday 1400 Friedman

Surveillance Gives Me Chills

Alex Marthews

In surveys, users say that government surveillance affects their online behavior, but users could always be lying. Join Alex as he takes you through the latest research on the effect of surveillance on actual user behavior - some of it his own - and connects this research to government and corporate efforts to chill and censor "extremist content" on the Internet.

Saturday 1000 Friedman

This Key is Your Key, This Key is My Key

Deviant Ollam, Howard Payne

We all know that the four most common passwords are love, secret, sex, and god. Like default passwords, locks are often keyed alike for convenience, perceived safety, or for economic and other reasons. This talk explores the idea of "popular keys" and how many lock systems are secured by easily guessable keys.

Sunday 1500 Lamarr

Movie: *Traceroute*

Johannes Grenzfurthner

Artist and lifelong nerd Johannes Grenzfurthner takes us on a personal road trip from the West Coast to the East Coast of the USA to introduce us to places and people that shaped and inspired his art and politics. *Traceroute* wants to chase and question the ghosts of nerd-dom's past, present, and future. An exhilarating tour de farce into the guts of trauma, obsession, and cognitive capitalism. The film features interviews with Matt Winston, Sandy Stone, Bruce Sterling, Jason Scott, Christina Agapakis, Trevor Paglen, Ryan Finnigan, Kit Stubbs, V. Vale, Sean Bonner, Allison Cameron, Josh Ellingson, Maggie Mayhem, Paolo Pedercini, Steve Tolin, Dan Wilcox, Jon Lebkowsky, Jan "Varka" Mulders, Adam Flynn, Abie Hadjitarkhani, and more.

A question and answer session will follow the film.

Friday 2200 Friedman (2 hours)

The TSA Keys Leak: Government Backdoors and the Dangers of Security Theater

DarkSim905, Johnny Xmas, Nite 0wl

In late 2015, hackers revealed yet another threat to American privacy, but this time it hit far closer to home than credit cards and Social Security numbers. The master keys the TSA uses to inspect all luggage being placed on an airplane were now available to anyone with a 3D printer! Three of the primary contributors to the leak and the subsequent reproduction of those keys will discuss their trials and tribulations during the event, including why government backdoors like key escrow are a *really bad idea,* the preposterousness of 3D printing keys in the first place, how the media completely missed the point of the entire operation, and how journalism doesn't actually even exist anymore. This will be a comprehensive discussion of literally every aspect of the TSA keys leak from top to bottom, including the release of previously undisclosed research. No talk of this magnitude has been given at any con on this topic! Notice: This talk will include the first public release of a *brand new master key!*

Saturday 2300 Lamarr

Tuning in to New York City's Pirates of the Air

David Goren

Pirate radio in New York City is a homegrown cultural phenomenon that is at once aesthetically vibrant, technologically tumultuous, and undeniably illegal. Emanating from clandestine studios and hidden transmitters, the sounds of Kreyol, Yiddish, Spanish, and Caribbean-accented English waft into the urban atmosphere. On an average night in Flatbush, Brooklyn, it's not uncommon to be able to hear as many as three dozen pirate stations between 87.9 and 107.9 Mhz. This flowering of outlaw micro-radio stations in Brooklyn and throughout the greater New York City region is a major disruption to the status quo of corporate controlled, robo-playlisted mega stations. Their unregulated presence and programming often reflects the throb and hum of a diverse city more authentically than traditional media outlets. Join radio producer David Goren for an audio tour of these stations featuring the music, programs, and personalities that make up New York City's pirate radio scene.

Friday 1900 Friedman

(CONTINUED ON PAGE 22)

FRIDAY

	Lamarr	Noether	Friedman
1000	Biology for Hackers and Hacking for Biology	The Phuture of Phreaking	
1100	I “Hacked” for China	What the Hack? Perceptions of Hackers and Cybercriminals in Popular Culture	How to Torrent a Pharmaceutical Drug
1200	When Vulnerability Disclosure Turns Ugly	Who’s Killing Crypto?	Matehacking: Legalizing Autonomous Production and Permaculture - Establishing a Hack Farm
1300	How Anonymous Narrowly Evaded Being Framed as Cyberterrorists	Only You Can Stop Police Surveillance - Here’s How	Show Networks
1400	The Panama Papers and the Law Firm Behind It: Shady Lawyers Caught With Their Pants Down	De-Anonymizing Bitcoin One Transaction at a Time	Is the Brain the Next Hackable Driver?
1500	Ask the EFF: The Year in Digital Civil Liberties	Your Level-Building Tool is Our Sound Stage	Chinese Mechanical Locks - Insight into a Hidden World of Locks
1600	The Onion Report	2016 Car Hacking Tools	What Really Happened? Fact, Truth, and Research Techniques
1700	Crypto War II: Updates from the Trenches	Censorship, Social Media, and the Presidential Election	Accessibility: A Creative Challenge to Living without Sight
1800	Privacy Badger and Panopticlick vs. the Trackers, Round 1	The Code Archive	How to Start a Crypto Party
1900	LockSport Roadshow: Bring Your Oddities!	Smart Cities and Blockchains: New Techno-Utopian Dreams or Nightmares?	Tuning in to New York City’s Pirates of the Air
2000	SecureDrop: Two Years on and Beyond	A Penetration Tester’s Guide to the Azure Cloud	Coding by Voice with Open Source Speech Recognition
2100	Slicing and Dicing Espionage: The Technical Aspect of Hunting Spies	Seven Continents: A Telecom Informer World Tour	Mesh VPN with Service Discovery
2200	Hacking Machine Learning Algorithms	National Security Letters: The Checks and Balances Aren’t Strong Enough - Sometimes They’re Nonexistent	Movie: *Traceroute*
2300	Eight Years of Radio Statler!	Security Options for High Risk Travelers	
2359	Movie: *Deep Web*	Open Mic	

SATURDAY

	Lamarr	Noether	Friedman
1000	Monitoring Dusty War Zones and Tropical Paradises - Being a Broadcast Anthropologist	Water Security: Are We in De-Nile or In-Seine? Water Policies, Availability, Geeks Without Bounds and You	Surveillance Gives Me Chills
1100	Leak Hypocrisy: A Conversation on Whistleblowers, Sources, and the Label "Espionage"	What is a "Neutral Network" Anyway? An Exploration and Rediscovery of the Aims of Net Neutrality in Theory and Practice	Orbital Mechanics Ate My Weblog
1200	Women in Cyber Security	Understanding Tor Onion Services and Their Use Cases	When Video Is Not Standard Output
1300	Keynote Address - Cory Doctorow		
1400			
1500	FOIA at Fifty	Medical Devices: Pwnage and Honeypots	Building Your Own Tor-centric ISP for Fun and (non)Profit
1600	Lockpicking in Real Life versus on the Screen	The Silk Road to Life without Parole - A Deeper Look at the Trial of Ross Ulbricht	Bring the Noise: Ten Years of Obfuscation as Counter-Surveillance
1700	Privacy, Anonymity, and Individuality - The Final Battle Begins	Detour Through Their Minds: How Everyday People Think the Internet Works	The Ownerless Library
1800		All Ages: How to Build a Movement	Computer Science Curricula's Failure - What Can We Do Now?
1900		Hacking Sex: Toys, Tools, and Tips for Empowerment and Pleasure	Won't Somebody Please Think of the Journalists?
2000	Stealing Bitcoin with Math	What the Fuck Are You Talking About? Storytelling for Hackers	Hacking DNA: Heritage and Health Care
2100	Social Engineering	Open Source Malware Lab	Social Engineering
2200	Now and Then, Here and There	Code Is from Mars, the Courts Are from Venus: Reverse Engineering Legal Developments on Reverse Engineering	Information Overload and the "Last Foot" Problem
2300	The TSA Keys Leak: Government Backdoors and the Dangers of Security Theater	CAPTCHAs - Building and Breaking	Attacking the Source: Surreptitious Software Features (and How to Become Extremely Paranoid)
2359	Movie: *Citizenfour*	Hackers Got Talent	

SUNDAY

	Lamarr	Noether	Friedman
1000	The Next Billion Certificates: Let's Encrypt and Scaling the Web PKI	Hackers Are Whistleblowers Too: Practical Solidarity with the Courage Foundation	Go Hack Yourself!
1100	LinkNYC Spy Stations	The Securitization of Cyberspace and Its Impact on Human Rights	FOIA and Public Records Hacking: How to Complete a FOIA Request or Dox Yourself via the Privacy Act
1200	Freedom and Privacy in Our Lives, Our Governments, and Our Schools	Iridium Satellite Hacking	Presidential Twitter Bot Experience
1300		Anti-Forensics AF	Censorship- and Coercion-Resistant Network Architectures
1400	Can We Sue Ourselves Secure? The Legal System's Role in Protecting Us in the Era of Mass Data Leaks and Internet of Things	Constructing Exocortices with Huginn and Halo	Sunset or Evolution of the PSTN?
1500	This Key is Your Key, This Key is My Key	Spy Hard with a Vengeance: How One City Stood up to the Department of Homeland Security	Hacking Housing
1600	The Black Holes in Our Surveillance Map	Come into My (Biohacking) Lab and See What's on the Slab	Democratizing Wireless Networks with LimeSDR: Open Source, Field-Programmable RF Technology
1700	The Mathematical Mesh and the New Cryptography	Hacking through Business: Theory and Logistics	Deconstructing Ad Networks for Fun and Profit
1800	Bringing Down the Great Cryptowall		
1900	Closing Ceremonies		

CODE OF CONDUCT

HOPE is dedicated to a harassment-free conference experience for everyone. The HOPE series of events are open, inclusive forums for sharing of ideas. HOPE participants include speakers, vendors, makers, tinkerers, families, students, and everyone else wanting to experience HOPE events and be part of the HOPE community. It is important for participants to step beyond prejudices, societal norms, and other perspectives that lead to disrespect for people and groups. Everyone is welcome to HOPE events, regardless of race, class, gender identity or expression, age, ethnicity, religion, political beliefs, disability, sexual orientation, personal appearance, or education level, text editor choice, and other aspects of who we are.

In short: HOPE is a space for tolerance and respect.
Our full anti-harassment policy can be found at xi.hope.net/codeofconduct.html
If you need to get in touch with a staff member during the event,
please call or text 929-325-2600, or email conduct@hope.net.

Anyone, press or otherwise, taking photos or videos of people at the conference must get consent. Likewise, if you accidentally take a photo or video and the person asks you to delete it, do so immediately. If you are taking "crowd shots," please announce your intentions to the crowd to allow people to look away.

TALKS (continued)

Understanding Tor Onion Services and Their Use Cases

asn, Nima Fatemi, David Goulet

In the last few years, we've seen more and more interest in Tor onion services (aka Tor hidden services). They are used by press to host whistleblowing platforms, by activists who want to set up a website that authorities want to shut down, by service providers to offer more security to their users, and for tons of other uses as well.

This panel will be presenting the technical aspects of Tor onion services as well as interesting use cases. As the onion service protocol aged, weaknesses started to appear in its design. For this reason, the speakers have been working since 2013 on the next generation onion service protocol. You'll get a status update on their progress, an explanation of the improvements it brings, and also why it is greatly needed.

Saturday 1200 Noether

Water Security: Are We in De-Nile or In-Seine? Water Policies, Availability, Geeks Without Bounds and You

Chris Kubecka, Lisha Sterling

The backbone of a modern society is clean, available water. Without clean water, production plants falter due to corrosion, lack of cooling capability, or unsteady supply. However, in many if not most parts of the world, water safety is a challenge. This presentation gives an introduction to some of these challenges, trying to ensure clean, available water and the consequences of unfiltered, dirty water. The focus is on what you can do to help solve this challenge. You, the technologist, the hacker, the lockpicker, the everyday person, can help devise better systems to solve some of these challenges. Geeks Without Bounds works around the world setting up solution-oriented hackathons that put participants in the driver's seat working together on technology issues to make the world a better place.

Saturday 1000 Noether

What is a "Neutral Network" Anyway? An Exploration and Rediscovery of the Aims of Net Neutrality in Theory and Practice

Jeremy Pesner, Kate Forscey, Bob Frankston, Sam Gustin, Alfredo Lopez, Jesse Sowell

This spring, the FCC's net neutrality rules were upheld in court, giving the commission license to regulate the Internet as a public utility and ensure that all users are treated fairly. However, the question remains as to exactly how net neutrality should be implemented and how well the concept applies to not only the Internet of today, but tomorrow. Panelists will discuss the tensions between applying the idea of net neutrality to the pragmatics of the Internet's operations and the very real social and policy consequences of such decisions. By combining and contrasting legal, activist, technical, journalistic, and academic perspectives, they will dig deep into the thoughts and aims behind net neutrality and derive a more nuanced and effective assessment of what is needed to create an Internet that works for everyone. The panelists have discussed, taught, and deliberated these issues in university, government, and social settings, and boast employment/affiliations with MIT, Harvard University's Berkman Center for Internet and Society, ACM, IEEE, Columbia University's School of Journalism, VICE Media, May First/People Link, and Public Knowledge.

Saturday 1100 Noether

What Really Happened? Fact, Truth, and Research Techniques

Evan Koblentz

Anyone can tell you something is true because they "researched" it. Evan will present some methods of performing historical research that stand up to challenges. Some of the methods are useful for social hacking, however the scope does not include any coding or technical subjects.

Friday 1600 Friedman

What the Fuck Are You Talking About? Storytelling for Hackers

Johannes Grenzfurthner

Humans are storytelling beings. From the moment the primordial ooze Mendelized itself into something like consciousness, we have been telling yarns: about the harvest, about the Gods, about the giant cats that wanted to eat us. But - for fuck's sake! - hackers are bad storytellers. Misunderstood by the media (and we're not even talking about the mainstream press!), ripped apart by their own peers, often incomprehensible and boring. But *whhhhyyyy???* What's going on in the hackersphere is probably shaping the future of our civilization. Narratology refers to both the theory and the study of narrative, and narrative structure and the ways that these affect our perception. You should come and listen, because it might save our movement - and more.

Saturday 2000 Noether

What the Hack? Perceptions of Hackers and Cybercriminals in Popular Culture

Aunshul Rege, Quinn Heath

How are hackers portrayed in the media? What are the typical stereotypes? How does the hacking community feel about the term "hacker," gender portrayals, and depictions in movies and television shows? This panel hopes to answer all of these questions and more!

Aunshul and Quinn were at HOPE X, talked to attendees then, and asked about their thoughts on the ways hackers were presented in the media. They are now back to share what they've found and to get more of your thoughts! Expect lots of interaction, conversation, and (possibly) heckling.

Friday 1100 Noether

When Video Is Not Standard Output

XioNYC

In a GUI-dominated cyberspace, the blind user is prey. When a UX change can mean the difference between productivity and disenfranchisement, when

an interstitial scareware alert is indistinguishable from a legitimate error dialog, and when security cannot be established because accessibility is left to the aftermarket, the frustrating onus upon a non-visual user exceeds the empowerment the sighted user takes for granted. This talk will shed light on some of these invisible "gotchas."
Saturday 1200 Friedman

When Vulnerability Disclosure Turns Ugly

Sam Bowne, Alex Muentz

Sam was accused of illegal hacking in the *SC Magazine* article "Professor Hacks University Health Conway in Demonstration for Class." That article made a mess so big, it took a real lawyer, Alex Muentz, to clear it up. Sam will explain how this happened and Alex will then explain how he handled this and offer informed advice on the laws around vulnerability disclosure, along with how to use the media effectively. In addition, Alex will describe a few other cases where attempts at responsible disclosure went wrong, what had to be done to fix it, and how the disclosure *should* have been done.
Friday 1200 Lamarr

Who's Killing Crypto?

Amie Stepanovich, Drew Mitnick

Governments have gotten really good at coming up with ways to undermine encryption. They can outright ban the use of certain types or strengths, place trade restrictions, mandate the insertion of backdoors or vulnerabilities, work with companies directly to undermine the encryption standards, arrest executives for failing to comply with orders, and seek assistance from courts through antiquated, off topic laws.

In this presentation, Amie and Drew will compare various approaches and provide the historical context that better illustrates how and why such restrictions are doomed to either fail or worsen the state of digital security. The session is planned to be part history lesson and part overview of the current state of encryption debates. The discussion will include where panelists think the law of encryption should and will go, and provide details on the campaigns that have been run at Access Now to promote the unrestricted use of encryption.
Friday 1200 Noether

Women in Cyber Security

Renee Pollark, Debora Gondek
Moderator: Cindy Cullen

With 11 percent of the cyber security workforce being women, why is it important to encourage women to be involved? How is security done differently by women or is it? This panel consists of women in different phases of career: just graduated college starting first professional job, mid-career, and experienced professional. Each panel member will provide an overview of their perspective on the workplace, including if they have experienced discrimination, how best to survive and thrive, and when it is time to move on.

Attendees will learn how others have responded to specific incidents, managed work life balance, become aware of how they may be making the environment feel hostile, and dealt with potential legal implications of their actions, and will also learn why having a diverse employee pool is good for the organization and for fellow employees.
Saturday 1200 Lamarr

Won't Somebody Please Think of the Journalists?

Tom Lowenthal

You'll never believe this one weird trick that lets you flip the script on mass surveillance. Oppressive institutions *hate* it. In this call to arms, we'll learn how to change up debates about secure software and fight calls for backdoors more persuasively, as well as develop a way of thinking about building and supporting tools which really serve people's security needs. The trick? Think (and talk) about journalists.
Saturday 1900 Friedman

Your Level-Building Tool is Our Sound Stage

Tamara Yadao, Chris Burke, Jeremy Pesner

Game art duo "foci + loci" (Tamara Yadao and Chris Burke) talk about hacking immersive video game spaces. Over the last six years, they have been using Little Big Planet to build and break custom game environments for live music performance. Joined by multidisciplinary technologist Jeremy Pesner, they will demonstrate and take apart some of their stranger maps and virtual instruments like the Tiltofon, the Flotrillium, and the Anytime-inator, while discussing successes and failures arising from repurposing or pushing game level-building tools beyond intended uses. They will raise questions about hacking the "look and feel" of game spaces and how it relates to professional game development tools like Unity and the Unreal Engine versus off-the-shelf games like *Little Big Planet, Minecraft,* or *Portal.* They will also look at Machinima (using game engines to create cinema) as an early strategy of video game appropriation and its relationship to culture jamming and hard/soft hacking in the gaming community. Lastly, they will present a sneak peak of the upcoming musical-in-game-space, *Songs from the Robot Apocalypse,* featuring the Arachnobot, the flying Toasterbot, and a robot made from a classic Game Boy DMG-1.
Friday 1500 Noether

The Budapest Option: Speakers often run out of time while the discussion is still going on. If they choose, they may invoke the Budapest Option, which means the conversation can continue in the Budapest room on the 6th floor after leaving the speaking area on the 18th floor. In the event that two or more talks invoke this option at the same time, the available time of one hour will be divided evenly. To get to Budapest, take the elevator down to the 6th floor, walk away from the elevators, and look to the right. There it is down the hallway.

SPEAKERS

aestetix served on the Oakland Domain Awareness Center ad hoc privacy committee as a technical expert. In addition, he has been involved in many privacy-aware projects, including Noisetor, the first nonprofit sponsored Tor exit node in the United States, and The Last HOPE and The Next HOPE badges, which involved RFID location-aware social networking. He also refuses to eat hot dog buns on Sundays, in accordance with the wishes of Our Goddess.

Salman Aljammaz is a programmer and occasional unicyclist. He's one of the developers of Camlistore, the content-addressed storage system on which The Code Archive runs.

Mitch Altman is a San Francisco-based hacker and inventor, best known for inventing TV-B-Gone remote controls, a keychain that turns off TVs in public places. He was also cofounder of 3ware, a successful Silicon Valley startup in the late 1990s, and did pioneering work in virtual reality in the mid-1980s. He has contributed to *Make Magazine* and other magazines, and wrote a chapter for *Maker Pro,* a book about making a living from projects one loves. For the last several years, Mitch has been giving talks and leading workshops around the world, teaching people to make cool things with microcontrollers, and teaching everyone to solder. He promotes hackerspaces and open-source hardware, and mentors others wherever he goes. He is a cofounder of the Noisebridge hackerspace in San Francisco, and is president and CEO of Cornfield Electronics.

Gillian "Gus" Andrews has been a senior usability research fellow at Simply Secure, continuing work she did on security usability at the Open Internet Tools Project. Her doctorate at Teachers College explored user misunderstandings of search. She has helped organize the HOPE conference since 2008, and has been a panelist on *Off The Hook.* She produces *The Media Show,* a series about media and digital literacy which has been featured on *Boing Boing,* the EFF blog, and Slashdot.

asn is a Tor developer and designer of high tech systems.

James M. Atkinson is a student, soldier, spy hunter, scientist, electronics engineer, computer programmer, cyber-operations specialist, computer and digital devices forensics... and a hacker and a phreaker since 1974. He is presently the president and senior engineer of Granite Island Group, a technical counterintelligence firm that specializes in the hunting of spies. He designs highly specialized equipment used to hunt spies.

Sean Auriti has skills in web development, engineering, and technical leadership. He graduated from NYIT with a BS in electronic engineering technology and has since worked as a CTO and lead developer at several web development and technology firms in New York City. He has won over 11 hackathons, including NYC BigApps and the BSR sustainability app. Sean has also founded, managed, and built infrastructure for the Alpha One Labs hackerspace, at which he has built prototypes for an LCD hat, laser scrolling sign, electronic game, 3D POV holographic display, robotic chef, smart recycle bin, and robotic food exchange. He was on the front page of *The New York Times* for a space group he was a part of that received DARPA funding.

Roni Bandini was born in Buenos Aires, Argentina and is a writer, journalist, and coder.

Zimmer Barnes served as hacker-in-residence at Tsinghua University in Beijing for six months, and went on to cofound Beijing's first feminist makerspace, Q Space. His previous projects include a wearable solar generator, a hydroponic system that cleans the air, his own recipe of chewing gum that makes you smarter, and segmented Kevlar rescue armor.

Burcu Baykurt is a doctoral student at Columbia University whose research interests are in the intersection of cultural sociology, urban policy, and media studies. Her dissertation examines the smart city experiments in U.S. cities, and how they are affecting civic culture, local politics, and urban inequality. Before coming to Columbia, she studied political communications at Goldsmiths, University of London and completed her MA in media, culture, and communication at New York University.

Beaches has been attending HOPE since HOPE Number Nine (2012). He has also been involved with Radio Statler since then.

Edward K. Beale is a retired U.S. Coast Guard O5, HH-65 helicopter aircraft commander, amateur radio technician (KC2GRD), author of *West By Sea,* regular stage speaker for eLearning Guild and numerous regional conferences, four-time expedition leader of helicopter support for polar ocean operations, and world traveler (Order of Magellan).

Charles Beckwith is a freelance executive and consultant, using his unique horizontal experience in fashion, media, and technology to help fashion and fashion-tech brands solve problems and build future-ready solutions. He is concurrently chief exploration officer at Open Source Fashion, and CEO of the Fashion Media Center think tank and marketing lab, where he is producer and co-host of the fashion industry's favorite show, *American Fashion Podcast.* A veteran media producer and artist with experience across radio, television, filmmaking, publishing, photography, theater, technology development, fiction writing, and live events management, he paints in his spare time.

Matt Blaze is a hacker and professor in the computer science department at the University of Pennsylvania. He's spoken at HOPE almost every time (he missed the second), and has testified before Congress on the issues presented in his HOPE talk this year.

Sam Bowne has been teaching security classes at City College in San Francisco since 2000. He has a PhD, a CISSP, and a lot of t-shirts.

Adam Brand has more than 12 years of experience in information technology and security. He is a director with Protiviti, where he has assisted companies in resolving major security incidents and maturing their information security programs. Adam has been heavily involved with the "I Am the Cavalry" movement, a group of researchers focused on information security issues that can affect human life and safety. He has recently focused on medical device security and is actively engaging with health care organizations on this issue.

John Brooks is the lead developer of Ricochet, a messaging system built on Tor hidden services, and a Tor core member.

Vivian Brown is a software engineer on EFF's web development team. She maintains eff.org and builds campaign sites and internal tools for EFF. Before joining EFF, Vivian was part of a worker co-op that provided web development and design services to social change organizations. Some of her other past projects include applying machine learning to birdsong and mapping Oakland campaign finance data.

William Budington is a security/software engineer at the EFF, where he works on Panopticlick, Open Democracy Tools, and other technology projects. As a crypto-enthusiast, he has contributed to many cryptography software projects such as SecureDrop and Let's Encrypt. He loves hackerspaces and getting together with other techies to tinker, code, share, and build the technological commons.

Bunni3burn is a homegrown Midwesterner hailing from a cornfield in Illinois, but ran away to a real city. She rarely sleeps, hardly leaves the house, and often forgets to eat. She enjoys pixel art, social engineering, and collecting bouncy balls. In kindergarten, Bunni3 played Ms. Pacman on a computer... and that's all it took. She fell in love with technology. Bunni3 has been around since the birth of Radio Statler at The Last Hope in 2008. She spent three years as the program director/producer. Now Bunni3 hangs around Radio Statler so she can take over the microphone after midnight.

Chris Burke has been creating peculiar media centered around games and game culture for 15 years, including the award-winning machinima talk show *This Spartan Life* and multiple chip music releases for 8bitpeoples, Astralwerks, and other labels under the name glomag. "Songs From The Robot Apocalypse" is his most recent project, expected to hit the stage later in the year.

Ebrahim Bushehri is the founder and CEO of the field-programmable RF chip company Lime Micro. He is also the founder of the nonprofit initiative MyriadRF, which seeks to bring open-source RF hardware to a wider audience through the development of low-cost, professional-grade hardware. Ebrahim's experience spans over 25 years in directing and managing of design teams for the implementation of high performance ICs within the wireless communication market. He has worked with organizations such as Nokia, Qinetiq (formerly Defence Evaluation Research Agency), and Fraunhofer IAF. Ebrahim is a member of the Institute of Electrical and Electronics Engineers (IEEE).

Matt Cagle is a technology and civil liberties policy attorney at the ACLU of Northern California, where he focuses on privacy, government surveillance, and free speech issues related to technologies used by businesses and governments. At the ACLU, Matt works on legislation affecting technology policy, promotes startup best practices, and collaborates with the litigation team. Prior to joining the ACLU as a policy attorney, Matt was an associate with BlurryEdge Strategies, a legal and business consulting practice providing legal advice to startups on products including connected devices, social networking platforms, and search services. With BlurryEdge, Matt worked extensively with companies fighting demands for user information and the removal of content, and he has authored multiple transparency reports. Matt is originally from Arizona, graduated summa cum laude with honors from the University of Arizona, and attended Stanford Law School.

Andrew Cantino is a software engineer who has worked at Google, Pivotal, and Mavenlink. In addition to cofounding BeeLine Reader, Andrew is also the creator of Huginn, an open-source workflow and integration engine that has more than 100 contributors and more than 13,000 stars on GitHub.

Ryan Castellucci has co-authored two papers about cryptographic attacks on Bitcoin and given talks on cracking brainwallets. For his day job at White Ops, he finds new and exciting ways to tease out the subtle differences between bots and human-controlled web browsers.

Kevin Chen is a biochemist and biohacker. He is a cofounder of Montreal's DIYbio community, Bricobio. When he's not working on the hacker/maker scene, he is working as the CEO and cofounder of Hyasynth Bio, a biotech startup that is producing cannabinoids using genetically engineered yeast.

The Cheshire Catalyst (Richard Cheshire) is the former publisher of the notorious *TAP Newsletter* of the radical 1970s and 80s. He has also attended (and volunteered at) every HOPE conference we've ever held. While available for speaking engagements, he is currently retired in Florida where he has his very own area code.

Ming Chow is a senior lecturer at the Tufts University Department of Computer Science. His areas of work are in web and mobile engineering and web security. He was a web application developer for ten years at Harvard University. Ming has spoken at numerous organizations and conferences.

Sandy Clark is a hacker and PhD candidate at the University of Pennsylvania. She studies the vulnerability life cycle, security vulnerabilities, and other interesting things.

Gabriella "Biella" Coleman holds the Wolfe Chair in scientific and technological literacy at McGill University. Trained as an anthropologist, her scholarship explores the intersection of the cultures of hacking and politics, with a focus on the sociopolitical implications of the free software movement and the digital protest ensemble Anonymous. She has authored two books, *Coding Freedom: The Ethics and Aesthetics of Hacking* and *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*, which was named to *Kirkus Reviews'* Best Books of 2014 and was awarded the 2015 Diana Forsythe Prize by the American Anthropological Association.

Naomi Colvin is a campaigner for the Courage Foundation, an international organization that supports individuals who risk life or liberty to make significant contributions to the historical record.

James Cropcho has been building software applications - and companies around those applications - for over a decade. He is the creator of the MongoDB schema analyzer Variety, which was featured on the official MongoDB blog in 2012. He was a member of the two-person team which uncovered the first wide-scale breach of the secret ballot in American history, and has been featured on National Public Radio and BBC News. Last spring, James designed and taught the graduate course "Web Development with Open Data" at New York University's Interactive Telecommunications Program.

Comet Crowbar is a queer white cis-lady, a self-published author and zinester, cofounder of the zine *Fest Berlin,* anti-imperialist, a member/organizer of the Uhuru Solidarity Movement, and a teacher at a DIY makerspace for kids called Parts and Crafts. She lives in so-called Cambridge, Massachusetts and runs a zine distro: Raumschiff Distro and Press.

Cindy Cullen has over 20 years of experience leading cybersecurity and information risk programs. Cindy is president of the New Jersey chapter of (ISC)2, is an ICIT fellow advising congress and staff on cybersecurity issues, and is chief cybersecurity strategist at HPE. Previously, she was CISO at Telcordia/Bellcore, vice president of IS at Citi, CTO at SAFE BioPharma, and designed an S-SDLC process for Bristol Myers Squibb. She served on the Bridgewater-Raritan Regional School Board for nine years, including as vice president and president.

DarkSim905 is founder of TOOOL New Jersey and has experience in instructing individuals on lockpicking, increasing their physical and virtual security posture. His particular interest is in bypass techniques and augmenting 3D designs to assist in generating keys for high security systems. Professionally, he is a sysadmin and Infosec goon. Curator of the #TSAkeys hashtag and living timeline, when not roaming the conference he can be found at the TOOOL lockpick village.

Benjamin Dean is a fellow for cyber-security and Internet governance at Columbia University's School of International and Public Affairs (SIPA). An economist by training, his research focuses on the economics of information, privacy, and data security. Benjamin worked on technology policy for three years in Paris, France, at the Organization for Economic Cooperation and Development (OECD). An Australian national, he has lived and worked in China, India, Bhutan, France, Venezuela, and the United States.

Molly de Blanc is interested in the intersections between society and technology, especially from the perspectives of ethics, community engagement, and practical implementation. At work, she is the community coordinator for the Open edX project at edX, and in her free time she is a free and open-source technology activist, Open Source Initiative board member, caretaker of plants and a cat, and rock star.

David Décary-Hétu earned his PhD in criminology from the University of Montreal in 2013. He has since worked and taught at the School of Criminal Sciences in Lausanne and the Polytechnique Engineering school of Montreal and is now an assistant professor at the School of Criminology of the University of Montreal. His main research interests are online illicit markets, especially those hosted on the darknet. The results of his research, funded by both the provincial and federal governments in Canada, have been published in major journals, have been presented at numerous conferences, and have been disseminated to a wide audience in a number of interviews with the media.

Fabrício do Canto is a "mate hacker" at metamate.cc and was an active member of the Pirate Party in Pankow, Berlin. He spent ten years on sabbatical traveling the globe with family realizing art and digital inclusion projects, mostly in India and other remote areas like Amazonia.

The Doctor is a security practitioner working for a currency remittance and financial software company on the West Coast. When not reading hex dumps, auditing code, writing bots to monitor critical business processes, or trying to break into his own networks from outside, he assists his local community however he can in making the world a better place, travels through time and space inside a funny blue box, contributes designs and code to a number of open-source hardware and software projects, and presents around the Bay Area on a number of technical topics. Exocortex, a software ecosystem for augmenting one's cognitive capabilities by farming out repetitive and tedious tasks that are still personally relevant, has been his skunkworks project for nearly 20 years and is now at the point where it should be usable by others.

Cory Doctorow (craphound.com) is a science fiction novelist, blogger, and technology activist. He is the co-editor of the popular weblog *Boing Boing* (boingboing.net), and a contributor to *The Guardian, Publishers Weekly, Wired,* and many other newspapers, magazines, and websites. (He even wrote an article for *2600* under a different name many years ago!) He is a special consultant to the Electronic Frontier Foundation (eff.org), you know, those superheroes who defend freedom in cyberspace on a daily basis. His two latest books are *In Real Life,* a young adult graphic novel created with Jen Wang (2014); and *Information Doesn't Want to Be Free,* a business book about creativity in the Internet age (2014). His latest young adult novel is *Homeland,* the best-selling sequel to 2008's wildly popular *Little Brother.* His latest novel for adults is *Rapture of the Nerds,* written with Charles Stross and published in 2012. His latest short story collection is *With a Little Help,* available in paperback, ebook, audiobook, and limited edition hardcover.

Ben Dubin-Thaler created the BioBus in 2007 to test his hypothesis that if people felt the excitement of scientific discovery, they would become more excited about doing science and becoming a scientist. This hypothesis has since been validated with 165,000 students from 500 schools boarding the BioBus and exhibiting dramatic positive changes in attitudes towards science and science careers. "Dr. Ben's" philosophy of providing hands-on, inquiry-based research lab experiences guides him as executive director of the nonprofit Cell Motion Laboratories, whose continuing mission is to create a future in which all people know the joy of scientific discovery through the construction of laboratory environments in which scientists join students for hands-on explorations of the natural world. Ben and his team recently created the BioBus Base, or "BioBase," a new community laboratory in Manhattan that is empowering, accessible, unintimidating, and facilitates in-depth scientific engagement even amongst populations historically underrepresented in science professions. He created the BioBus after completing his BA in physics and mathematics, as well as his PhD in biology from Columbia University. The author of numerous high-profile research articles and book chapters in cell biology and biophysics, Dr. Ben has lectured at the American Society for Cell Biology, the National Institutes of Health, Rockefeller University, New York University, the University of Illinois, PopTech, TEDxWoodsHole, and the Materials Research Society, receiving numerous awards and accolades for excellence in research and teaching.

Jameson Dungan is a self-taught biohacker and founder of Biologik Labs in Norfolk, Virginia. He is passionate about maker/hacker culture, urban exploring, and cyberpunk art. While democratizing science and teaching biology, he is also a supporter of open-source hardware and learning by doing.

Scott Erven is an associate director at Protiviti. He has over 15 years of information security and information technology experience with subject matter expertise in medical device and health care security. Scott has advised the U.S. Department of Homeland Security, Food and

Drug Administration, and national policymakers. His research on medical device security has been featured in *Wired, Forbes,* BBC, and numerous media outlets worldwide. He has presented his research and expertise in the field internationally. His current focus is on research that affects human life and public safety issues inside today's health care landscape.

Eric Evenchick has worked at several automotive companies and is the creator of the CANtact CAN bus sniffer.

Mark Fahey lives in Sydney, Australia and is a biomedical informatics specialist who develops acute-care clinical solutions. His other current projects include *Behind the Curtain,* a multimedia and print analysis of North Korean propaganda and mind control techniques; Satdirectory, a free-to-air satellite directory; and MediaExplorer, a virtual travel guide to free-to-air digital satellite reception of information about remote lands and intriguing cultures.

Nima Fatemi is an Iranian independent security researcher, focused on encryption, anonymity, privacy, and censorship circumvention technologies. He is a core member of The Tor Project and the chief technologist of Library Freedom Project.

Kate Forscey joined Public Knowledge as an Internet Rights Fellow in April 2014, and transitioned to her role as Associate Counsel for Government Affairs in April 2015. Kate advocates for the public interest on Internet and technology policy and government affairs, including net neutrality, video and broadband competition, spectrum policy, and other issues crucial to preserving an open Internet and consumer digital rights. Prior to joining PK, Kate worked on Internet and technology issues for the Open Internet Coalition as a summer associate for Holch and Erickson, focusing primarily on the FCC's 2010 open Internet proceeding. Kate received her JD from Vanderbilt University Law School in 2012 and holds a BA in psychology with a focus in psychobiology from the University of Virginia College of Arts and Sciences.

Camille Francoise is a fellow at Harvard Law School's Berkman Center for Internet and Society, and at the Yale Law School Information Society Project. A Fulbright fellow, she is also a visiting scholar at Columbia University's Saltzman Institute of War and Peace Studies, where she consulted for the U.S. Defense Advanced Research Projects Agency (DARPA) on cybersecurity.

Bob Frankston was born in Brooklyn, New York, graduated from MIT in Cambridge, Massachusetts with degrees in computer science and electrical engineering, and is on the Board of Governors and is a Distinguished Lecturer for the IEEE Consumer Electronics Society. He has been online since 1966, was co-developer of the first electronic spreadsheet (VisiCalc), and has been honored by the IEEE for his contributions to home networking while at Microsoft. At Microsoft, he took the initiative to give people control of their home networking and developed the worldwide standard for how we connect our computers to the Internet. Since leaving Microsoft, Bob has done angel investing, consulting, and advising, and currently works with entrepreneurs and established companies on the issues we face as we transition to a software-defined connected world.

Limor "Ladyada" Fried is founder and engineer of New York based Adafruit Industries. Limor started Adafruit in 2005 while at MIT studying engineering. Her goal was to create the best place online for learning electronics for makers of all ages and skill levels. Adafruit has grown to over 100 employees in the heart of New York City with a 50,000 plus square foot factory. Limor was the first female engineer on the cover of *Wired Magazine* and was awarded *Entrepreneur Magazine's* Entrepreneur of the Year. Ladyada was on the New York City Industrial Business Advisory Council and Adafruit was ranked Number 11 in the top 20 USA manufacturing companies and number one in New York City by *Inc. Magazine's* 5000 fastest growing private companies.

Jared Friend is a senior privacy and technology attorney at Hintze Law. His representative areas of experience are free/open-source licensing and compliance, online and mobile tracking, FTC inquiry and order compliance, regulatory data security compliance, development of internal privacy and data security practices, biometrics, and regulatory policy. Jared was formerly the director of the Technology and Liberty Program at the ACLU of Washington, where he was responsible for driving policy work at the intersection of free speech, privacy, and developing technology and for collaborating with the policy and litigation teams throughout the ACLU. Jared attended Berkeley School of Law, where he received the Law and Technology Certificate, worked for the Samuelson Technology Clinic, and was a member of the Berkeley Technology Law Journal submissions team. Prior to law school, Jared worked for a number of technology companies in the Seattle area in test engineering roles.

Nathan Fuller is a writer based in New York City. Before joining Courage, he covered Chelsea Manning's trial for her support network.

Emmanuel Goldstein was responsible for editing all of these bios and was, ironically, completely unable to write one for himself.

Fred Goldstein advises governments and companies on technical, regulatory, and business issues related to the telecommunications, cable, wireless, and Internet industries, especially in areas where they overlap. He assists service providers in network design, business modeling, planning, and technical architecture. He helps municipalities develop their own networks, fiber and wireless, to bring broadband services to unserved areas. He has frequently been an expert witness in patent, regulatory, and telecom disputes. He has worked with enterprise networks on a wide range of matters such as backbone network design, voice systems planning, and traffic engineering. The author of numerous articles and the books *The Great Telecom Meltdown* and *ISDN In Perspective,* he has served on standards committees in areas such as ATM networks and frame relay, and has taught courses on various telecom-related subjects.

Debora Gondek is an operational risk manager experienced in assessing information security risk across the application development life cycle. She's worked for several financial services organizations, including Citi, HSBC, and Bear Stearns. Early in her career, she managed a lab where emerging network engineering solutions were evaluated. Later, she helped establish an ethical hacking program at a global bank. She currently designs tools and procedures to measure and manage technology risk.

David Goren is a radio producer and audio archivist with a focus on broadcast culture. His work has been featured on NPR's *Lost and Found Sound* series, *On the Media, Afropop Worldwide, Jazz at Lincoln Center Radio,* and shortwaveology.net.

David Goulet is a Tor developer and a developer of Off-the-Record (OTR), which provides end-to-end encryption for IM.

Andy Greenberg is a reporter for *Wired,* where he writes about information security, privacy, cryptography, and hacker culture. He's the author of the book *This Machine Kills Secrets,* on the history and future of anonymity, the cypherpunks, and information leaks. In 2013, he conducted the media's only extended interview with the Dread Pirate Roberts, the administrator of the Silk Road dark web black market.

Johannes Grenzfurthner is an award-winning director, artist, writer, and researcher. He lives and works in Vienna, Austria and Durango, Colorado in the USA. He is the founder and artistic director of monochrom, an internationally-acting art and theory group. He likes to engage in "urban hacking," or, more specifically, "context hacking," a term that Grenzfurthner coined. He directed the dark sci-fi comedy *Die Gstettensaga: The Rise of Echsenfriedl,* the feature documentary *Traceroute,* and is currently working on several other movie projects (*Tycho!, Sierra Zulu, Nothing To Hide*). He is one of the most outspoken researchers in the field of sexuality and technology, and one of the founders of "techno-hedonism." He is head of Arse Elektronika (sex and tech festival) in San Francisco, Hedonistika (food tech festival in Montreal and Tel Aviv), and host of Roboexotica (festival for cocktail-robotics) in Vienna. He teaches art theory and art practice at the University of Applied Sciences in Graz, Austria, and is a lecturer on culture jamming at the University of Arts and Industrial Design in Linz, Austria.

Sam Gustin is a journalist focused on the intersection of business, technology, media, and public policy. He is currently a correspondent at *Vice Motherboard* and previously worked for *Time, Wired,* and other publications, where he reported on the nation's largest technology and telecom companies and their relationships with the government. He has a master's degree in journalism from Columbia University and a BA in political science from Reed College. From 2014 to 2015, Sam was a fellow at the Berkman Center for Internet and Society at Harvard University, where he focused his research on U.S. communications policy, with a particular emphasis on community broadband networks.

Phillip Hallam-Baker has been involved in web security since 1992. He was responsible for security issues in the CERN web team and took the payments brief at the newly formed Web Consortium at MIT. After a spell working on the security of an email system deployed in the Clinton-era Executive Office of the President at the MIT AI Lab, he joined VeriSign where he spent 12 years as principal consultant. He currently divides his time between working as vice president and principal scientist at Comodo and as an expert witness in Internet-related cases. He has played a leading role in the development of many Internet standards, in particular, the WebPKI which is the certificate authority run infrastructure that provides credentials for SSL/TLS, SAML and XKMS. He is a member of the IETF Security Area Directorate and holds eight U.S. patents.

Quinn Heath is an undergraduate student studying computer science and criminal justice at Temple University. He has had an interest in computers and hacking since high school, particularly in the study of cybercrime and computer forensics. This is Quinn's first HOPE and first time speaking at a hacking conference.

Weston Hecker has spent 11 years pen-testing and 12 years performing security research and programming. He has worked with a major university and the Department of Homeland Security on 911 emergency systems and attack mitigation. He has found several vulnerabilities in very popular software and firmware, including Microsoft, Qualcomm, Samsung, HTC, and Verizon.

Caitlin Kelly Henry is a Bay Area based attorney and professor. Her practice includes FOIA, watch-list investigations, business formation, and work with incarcerated people.

Michael Hernandez is a Brooklyn born RYT200 certified yoga teacher with plans to get 500 hour certification this year. He's been a software engineer at Etsy for the last five years, and a hacker of a sort for his entire life.

Parker Higgins is an activist at the Electronic Frontier Foundation, specializing in issues at the intersection of freedom of speech and copyright, trademark, and patent law. As a participant in EFF's Apollo 1201 project, he is helping Cory Doctorow to eliminate DRM in our lifetime. He previously lived and worked in Berlin, Germany.

Mariko Hirose is a senior staff attorney at the New York Civil Liberties Union, where she has worked on issues involving free speech, privacy, government transparency, and criminal justice. She previously served as a fellow at the Speech, Privacy, and Technology Project of the American Civil Liberties Union. She is also an adjunct professor at the Fordham University School of Law, where she teaches a course on privacy and surveillance in the digital age. Mariko is a graduate of Yale University and Stanford Law School.

Brian Hofer is a member of the Oakland Privacy Working Group, which formed to oppose the Domain Awareness Center. He chaired the DAC ad hoc privacy committee, which has since introduced two City Council adopted privacy and data retention policies, along with an ordinance making the privacy committee permanent.

Jacob Hoffman-Andrews is a lead developer on Let's Encrypt, the free and automated certificate authority. He also works on EFF's Encrypt the Web initiative and is a maintainer on the HTTPS Everywhere browser extension. Prior to working at EFF, Jacob was on Twitter's anti-spam and security teams. On the security team, he implemented HTTPS-by-default with forward secrecy, key pinning, HSTS, and CSP. On anti-spam, he deployed new machine-learned models to detect and block spam in real time. Before Twitter, he worked at Google, variously on the maps, transit, and shopping teams.

Sebastian Holst is chief strategy officer at Preemptive Solutions, makers of application security and analytics products. Over the last 20 years, Sebastian has held leadership positions in risk management, content management, and database software companies. In addition, he has worked to promote computing and industry standards, serving on the W3C Advisory Committee, ActOnline.org, OCEG.org, and as an IDEAlliance board member. Sebastian most recently testified on privacy and IP topics before the U.S. Senate Judiciary Committee. He also lends his time to a boutique cybersecurity firm that he cofounded and to TheMobileYogi, a mobile app portfolio company cofounded with his wife.

Joshua Horowitz's practice is concentrated on litigation matters requiring expertise in technology and computer software. He has served as the technology lawyer on the defense team of multiple federal cybercrime cases in the Southern District of New York, including the Silk Road trial (United States v. Ulbricht) and other international cybercrime matters. He also represents corporate clients in government investigations involving technologically complex legal issues. In the Silk Road case, he submitted an 18-page declaration undermining technical assertions made by the FBI with regard to their discovery of computer servers located abroad. His work raised significant questions about the government's purported methodology in uncovering computer servers hosted as a Tor hidden service, receiving national recognition in *Forbes, Wired, TechCrunch, Ars Technica,* and other publications. While in law school, Joshua worked at the Software Freedom Law Center, an organization providing legal counsel to Free and Open Source (FOSS) software developers in a broad variety of legal matters. He received his BA from the University of Rochester and JD from Ohio Northern University and launched his practice immediately upon graduating from law school.

Daniel C. Howe is an artist, researcher, and critical technologist whose work focuses on the social and political implications of networks and computational technologies. He has a PhD in computer science and currently lives in Hong Kong, where he teaches at the School of Creative Media.

John Huntington is a professor of entertainment technology at New York City College of Technology (Citytech/CUNY) and also works as an entertainment technology and show control systems consultant, author, and sound designer/engineer. He blogs about entertainment technology at www.controlgeek.net, chases tornadoes in his spare time, and sells photos on www.johnhuntington.photography.

int0x80 is the rapper in Dual Core. Drink all the booze, hack all the things!

Luke Iseman and **Heather Stewart** live in homes they've built out of shipping containers in the East Bay. They have a negative cost of living monthly, and they think everyone should spend more time building big things out of metal. Luke spends his spare time prototyping hardware and Heather makes giant art.

Jameel Jaffer is a deputy legal director of the National ACLU and Director of the ACLU's Center for Democracy, which houses the National ACLU's work relating to free speech, privacy, technology, national security, and international human rights. He has argued cases in multiple appeals courts, as well as in the U.S. Supreme Court, and he has testified before Congress on several occasions concerning issues relating to counterterrorism policy and civil liberties. He co-led the Freedom of Information Act litigation that resulted in the release of the Bush administration's "torture memos." More recently, he led the ACLU's litigation that resulted in the release of some of the Obama administration's "drone memos."

Joshua is a red teamer and former infantryman who thoroughly enjoys getting into an attacker mindset.

Tom Keenan wrote his first computer program in 1964, worked on some of the earliest timesharing systems, and taught Canada's first computer security course. He is the author of the best-selling book *Technocreep* and a frequent guest on radio and television. He loves to get people excited and riled up about cool things.

Paul Kernfeld is a software engineer and peer-to-peer systems enthusiast.

Mallory Knodel is the technology policy lead and sysadmin for the Association for Progressive Communications (APC), a member of May First/People Link's steering committee, and on the executive board of eQualit.ie.

Evan Koblentz is a technology journalist and president of the nonprofit Vintage Computer Federation.

Bethany (Benny) Koval was a household name for just about 15 minutes when, with the help of the ACLU, she successfully battled her school's administration over her constitutional right to say "Fuck Israel" on Twitter. Within those 15 minutes, Zionists held peaceful rallies against her, vandalized her house, and her friends abandoned her. But this just made her more motivated to speak out against all injustice. She's both elated and honored to join the Four Thieves Vinegar Collective in their fight against injustice as well, and plans to fight the injustice of the prison industrial complex by becoming a criminal defense attorney in the future.

Spencer (nibalizer) Krum has been sysoping Linux since 2010. He works for IBM, contributing upstream to OpenStack and Puppet. Spencer coordinates the local DevOps user group in Portland and volunteers for an ops-training program at Portland State University called the Braindump. Spencer lives and works in Portland, Oregon where he enjoys tennis, cheeseburgers, and StarCraft II.

Chris Kubecka, owner of HypaSec, currently advises several governments on their critical infrastructure with a focus on water, oil and gas, and nuclear industries. She is the former group leader of Aramco Overseas in The Netherlands and led their security operations center. She holds degrees in aeronautical engineering, computer science, and information technology. Chris holds an alphabet soup of certifications. Her hobbies include research of smartphone/Android OS exploitation, cyber warfare, process and automated control systems, DNS and IPv6 protocols, cryptography, SIEM's/correlation engines, and cyber-intelligence. Chris has over 20 years of extensive experience in the field of information security. Her career has spanned from the U.S. Air Force, Space Command, and the private and public sector.

Ryan Lackey has been involved in computer security since discovering the cypherpunks mailing list in the early 1990s. He founded the world's first offshore datahaven (HavenCo) and then spent a decade building satellite and wireless communications networks in conflict zones in the Middle East. After returning to the U.S., he founded CryptoSeal, a server-side tamper-resistant computing company which also operated a VPN, which he sold to CloudFlare in 2014. He now is founder of Travel Fleet, a startup solving travel security problems for corporate executives and professionals going to high risk environments around the world.

Michael Swan Laufer worked in mathematics and high energy physics until he decided to use his background in science to tackle problems of world health and other social issues. Perpetually disruptive, his most recent project makes it possible for people to manufacture their own medications at home. Open-source, and made from off-the-shelf parts, the Apothecary MicroLab puts many medications within the reach of those who would otherwise not have them.

Mathieu Lavoie recently graduated from ETS and works as a pentester for a large financial institution. He previously worked as a malware researcher at ESET and as a computer security freelancer. During his free time, he is an avid participant to many CTFs in the infamous CISSP Groupies (now called DCI-ETS), where he developed a deep love-hate relationship with crypto challenges or Defcon's so-called "web" challenges. As such, he was multiple times a finalist at the CSAW competition, and can even be seen somewhere on their website (no points for this flag). He speak at some local conferences including the first NorthSec conference in Montreal.

Timothy Libert is a doctoral candidate at the Annenberg School for Communication at the University of Pennsylvania and a research fellow at the Alexander von Humboldt Institute for Internet and Society in Berlin. His research focuses on privacy-compromising information flows on the web, and he is the author of the open-source software platform webXray. He has published work in *The Communications of the Association for Computing Machinery, The International Journal of Communication,* and *The BMJ* (British Medical Journal). His work has received international press coverage and he has been interviewed by National Public Radio's *All Things Considered, Good Morning America,* and other outlets. His publications may be downloaded at his personal website: https://timlibert.me.

Gareth Llewellyn moves packets around the Internet for a living, is a technical volunteer for the OpenRightsGroup (e.g. helping to design and build www.blocked.org.uk), and founder of Brass Horn Communications.

During his nearly half-century career of movement activism, organization, and writing, **Alfredo Lopez** has been a leader in the Puerto Rican independence, labor, and antiwar movements, an organizer of several major national demonstrations and scores of smaller ones, editor of two publications (*Claridad* and *Sevendays Magazine*), a radio and television producer/host, a college professor, and author of six published books and hundreds of published articles. He is a founder and leader of May First/People Link, the largest political progressive Internet membership organization in the U.S., and in that capacity he has helped shape much of May First's service provision system (including the 130 virtual server system shared by May First members), helped develop the organization's how-to and help systems, and participated in developing its suite of free and open-source software that the organization makes available to its members. Alfredo is a prominent leader in the struggle over net neutrality and has organized rallies, teach-ins, and congressional lobbying visits to push for its protection, and writes extensively on issues like privacy, data protection, net neutrality, and open access for the online publication *This Can't Be Happening*. He currently serves on the board of the Center for Media Justice, is a member of the steering committee of MAGNet (the Media Action Grassroots Network), and is a member of the National Planning Committee of the U.S. Social Forum.

Lauri Love is a British activist, part of the 2011 Hetherington House Occupation, who is charged with breaching multiple U.S. government computers. He is currently fighting extradition to the United States (which is why he will be on a video link).

Tom Lowenthal is a technologist and activist committed to combating our contemporary cyberpunk mass-surveillance dystopia. By day, he's the staff technologist for the tech program at the Committee to Protect Journalists. By night, he practices healthy self-care because mental health is really important and burnout can be a killer. Tom's also a fellow at Stanford's Center for Internet and Society; he's previously worked at the Tor Project and Mozilla. He's a big believer in individual privacy, self-determination, and practical usable tools.

Nick Lum is a jack of a few trades and master of none. After spending several years in corporate America, Nick launched BeeLine Reader (somewhat by accident) on Hacker News. Since dedicating himself full-time to this startup, it has won social entrepreneurship awards from Stanford University and The Tech Museum of Innovation.

Alex Marthews is the national chair of Restore The Fourth, an anti-surveillance movement with chapters across the country. Alex holds a master's degree in public policy from UC Berkeley, and used to intern at EFF back when it was small.

Apostolos Mastoris is an ethical hacker working as a security consultant at MWR InfoSecurity in London. His interest in security began when he was involved in the *2600* meetings in Athens, Greece. His day-to-day activities include application and infrastructure penetration testing and consulting clients on ways to improve the security of their environments. He holds a BSc in computer engineering and an MSc in information security. In his free time (when there's any), he enjoys reading recent updates in the security community, doing some coding, and getting involved in problem solving activities.

Janine Medina is a biohacker working in health care analytics and business intelligence who practices alchemy.

Manos Megagiannis, CTO of Black Chambers Inc., has been involved with *2600* in one way or another since the 1990s. Manos has over 20 years of professional experience with Infosec in several key areas, including investigations, offensive and defensive tactics, LAN/WAN architecture, secure voice and data communications, and due diligence and vetting of commercial solutions. He has consulted for many Fortune and Global 500 companies, and has been responsible for the conceptualization, design, and implementation of security applications and has helped set industry standards for computer networks. His work has received commendations from federal, state, and local governments. Manos holds both a BS and master's degree in computer science from the City University of New York.

Nicholas Merrill is the executive director of The Calyx Institute, a nonprofit educational organization based in New York City. Prior to founding The Calyx Institute, he founded one of the first Internet service providers in New York: Calyx Internet Access in 1994. In 2004, he began a 12-year legal challenge to National Security Letters, and their unconstitutional searches and "gag orders" - another term for non-disclosure orders.

Stefania Milan holds a PhD in political and social sciences of the European University Institute in Italy, and is the author of *Social Movements and Their Technologies: Wiring Social Change,* and co-author of *Media/Society.* Currently, she is assistant professor at Tilburg University in The Netherlands and the founding director of the Data J Lab, focusing on big data analytics. Stefania serves in the executive committee of the NonCommercial Users Constituency of the Internet Corporation for Names and Numbers (ICANN) and in the /1net Steering Committee.

Drew Mitnick focuses on digital security, digital due process, and privacy. He has experience working on human rights in Asia and the United States.

Alex Muentz is both an information security consultant and a lawyer with a fondness for seersucker in this heat. He's spoken at a bunch of conferences you've heard of (HOPE, Defcon, ShmooCon). He occasionally takes pro-bono cases and attempts to avoid career-limiting moves.

In addition to being co-editor for cryptome.org, **Deborah Natsios** is responsible for the associated project Cartome, which was founded in 2011, and posts her original critical art and graphical images and other public resources to document sensitive areas. She additionally holds a degree in mathematics from Smith College.

Deb Nicholson wants to make the world a better place with technology and social justice for all. She likes talking to developers about software patents, to project maintainers about leadership, and to activists about free software. In the service of worldwide free software promotion, she is a prolific speaker, writer, and both IRL and IRC meeting attender. When she's at home in Massachusetts, she volunteers for Girls Rock Campaign, haunts the science fiction book store, and keeps a small herb garden.

Nikgod is a reformed network engineer who occasionally pretends to know how radio works. Once he figured out how to hack AOL 2.0 parental controls, the Internet scarred him for life. Nikgod functions as the chief engineer of Radio Statler, coming up with solutions to the hard technical problems and running up a tab on his credit cards in the process.

Nite 0wl has been picking and bypassing locks since kindergarten and continues to do this at his own expense. He has spoken on communications and physical security at *The New York Times* as well as at various less formal events. You may have recognized him in his recurring role as "sleep deprived volunteer who is outweighed by his beard" at previous HOPE conferences or at various TOOOL lockpicking villages.

Grace North is a prisoner support activist who leads Jeremy Hammond's support network and has advocated for prisoners' rights for years.

Deviant Ollam is a member of the board of directors of The Open Organisation Of Lockpickers (TOOOL) in the United States. Growing up with James Bond films and the TV show *I Spy,* he was fascinated with lockpicking from a young age, but never really got deep into this topic until witnessing TOOOL members firsthand at HOPE. He now helps to run the lockpick village at many cons around the world, has published books, and has visited over 100 cities across 17 countries teaching about lockpicking.

Patrick Howell O'Neill is a journalist at *The Daily Dot.* He reports on politics, technology, and security.

Kurt Opsahl is the deputy executive director and general counsel of the Electronic Frontier Foundation. In addition to representing clients on civil liberties, free speech, and privacy law, Kurt counsels on EFF projects and initiatives. He is the lead attorney on the Coders' Rights Project. Before joining EFF, Kurt worked at Perkins Coie, where he represented technology clients with respect to intellectual property, privacy, defamation, and other online liability matters, including working on Kelly v. Arribasoft, MGM v. Grokster and CoStar v. LoopNet. For his work responding to government subpoenas, he is proud to have been called a "rabid dog" by the Department of Justice. Kurt received his law degree from Boalt Hall and undergraduate degree from U.C. Santa Cruz. He co-authored *Electronic Media and Privacy Law Handbook.* In 2007, Kurt was named as one of the "Attorneys of the Year" by *California Lawyer* magazine for his work on the O'Grady v. Superior Court appeal. In 2014, he was elected to the USENIX Board of Directors.

Shaf Patel is a blind locksmith and tech enthusiast from London, U.K. He has a passion for cyber security, coding, encryption, social engineering, disability advocacy, and human rights. He also enjoys partaking in passionate debates and is always open to new ideas and opportunities.

Howard Payne is an elevator consultant with a strong interest in locks and physical security. He is a proponent of freedom of information laws, and an opponent of open standards that call for specific key combinations (especially when it pertains to elevators).

Ellen Pearlman is a PhD candidate at The School of Creative Media, Hong Kong City University. She is director and curator of the Volumetric Society of New York, a 2400 member organization, and president of Art-A-Hack, which brings artists and technologists together to make something new.

Jeremy Pesner is a multidisciplinary technologist, researcher, policy analyst, and gamer who holds a BS in computer science from Dickinson College and an MA in communication, culture, and technology from Georgetown University. He is fascinated by questions and implications of technology, media, and games across entertainment, education, and the blending of arts and science. He has worked for educational games company E-Line media and helped to run the Music and Gaming Education Symposium at the Music and Gaming Festival for the past six years, where he has spoken and demonstrated extensively on how to evaluate player experiences in video games. He is also passionate about other technology issues like broadband, technological innovation, and how technology can make a positive difference in lives throughout the world.

Ed Platt makes technology and communities, often at the same time. He is currently doing PhD research on decentralized communities at the University of Michigan School of Information. Before coming to UMSI, he cofounded the i3 Detroit hackerspace and worked as a researcher at the MIT Center for Civic Media.

Kyle Polich has been a data scientist for over a decade. He hosts the *Data Skeptic* podcast that explores the intersection of data, machine learning, statistics, and scientific skepticism.

Renee Pollark is a Blackstone security consultant who has researched mobile malware and vulnerabilities in applications and cellular networks.

Max Power is one of TOOOL's most active and level-up members. When he's not powerlifting padlocks in order to see just how much weight his adamantium reinforced bones can bear, he's methodically polishing the pick tools that can extend from his knuckles like claws for attacking deadbolts and door locks. If you see Max, either steer clear or give him a splendid high five and ask how his local Boston sports teams are doing... because no one from The City on The Hill will miss a chance at that discussion. (Max didn't write this bio but he supremely likes the fellow who did.)

David Pozen is a professor at Columbia Law School. A former special assistant to Senator Edward M. Kennedy and law clerk to Justice John Paul Stevens, he has written widely on government secrecy and on constitutional law and theory. His recent academic articles include "Privacy-Privacy Tradeoffs" (*University of Chicago Law Review*), "Uncivil Obedience" (*Columbia Law Review*), and "The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information" (*Harvard Law Review*).

Cooper Quintin is a security researcher and programmer at EFF. He has worked on projects such as Privacy Badger, Canary Watch, Ethersheet, and analysis of state sponsored malware. He has also performed security trainings for activists, nonprofit workers, and ordinary folks around the world. He previously worked building websites for nonprofits such as Greenpeace, Adbusters, and the Chelsea Manning Support Network. He also was a cofounder of the Hackbloc hacktivist collective. In his spare time, he enjoys playing music and participating in street protests.

Jesselyn Radack is an attorney and director of the Whistleblower and Source Protection Program (WHISPeR) at ExposeFacts. She is a former Justice Department whistleblower, representing Edward Snowden, Thomas Drake, and numerous drone pilot whistleblowers.

Steven Rambam is the founder and CEO of Pallorium, Inc., a licensed investigative agency with offices and affiliates worldwide. Steven has coordinated investigations in more than 60 countries, and he specializes in international and multi-jurisdictional investigations, investigations of sophisticated frauds, and missing person investigations. Many of Steven's activities involve coordination with national authorities, and Steven has received commendations and awards in a number of foreign locations. He has also received a number of foreign military decorations, and his activities have been mentioned in sessions of the Canadian and Israeli Parliaments. Steven is perhaps best publicly known for his pro bono activities, which have included the location and investigation of nearly 200 Nazi collaborators and war criminals in the USA, Canada, Europe, and Australia. He has also coordinated efforts to expose terrorist groups' fundraising activities in the United States and has conducted investigations which resulted in the tightening of airport security in eight U.S. cities. He has been the host of Discovery ID's *Nowhere To Hide* and History Channel's *Hunting* reality television shows, and is scheduled to host "Private Justice" TV. (*Nowhere To Hide* premiered at HOPE X and past episodes are available via iTunes, Amazon, and, undoubtedly, Kickass Torrents.) Steven has presented at every HOPE since Number One.

Aunshul Rege is an assistant professor in the criminal justice department at Temple University. Trained as a criminologist, some of her research interests include critical infrastructure cyberattacks; cybercrimes against gambling and dating websites, understanding how migrant women in IS use social media, and interacting with the hacking community at large.

Garrett Robinson is the CTO at Freedom of the Press Foundation and the lead developer of SecureDrop. His interest in empowering whistleblowers through technology began when he was involved with environmental activism in Appalachia, and that led to the creation of a whistleblower submission site called Honest Appalachia. He previously worked full time as a security and privacy engineer for Mozilla, and also for the Electronic Frontier Foundation.

schneider is an embedded software and hardware developer and member of the Munich Chaos Computer Club group. He likes to hit the "Remote Update" button for thousands of devices every now and then.

Jason Scott's official title at the Internet Archive is "free-range archivist," which means he spends a very large amount of time acquiring a very large amount of data. He founded textfiles.com in 1998 and continues to warp minds daily as a result.

Carey Shenkman is a First Amendment and human rights attorney with the Center for Constitutional Rights representing journalists, including Julian Assange and WikiLeaks.

Elissa Shevinsky is a serial entrepreneur and an activist on behalf of transparency and free speech. Recent work includes building end-to-end encrypted applications such as Glimpse, and being head of product at Brave Software. She is also the editor of *Lean Out,* published by OR Books.

Robert Simmons is a senior threat intelligence researcher at ThreatConnect, Inc. With an expertise in building automated malware analysis systems based on open-source tools, he has been tracking malware and phishing attacks and picking them apart for years. Robert is also the author of PlagueScanner, an open-source virus scanner framework.

Craig Smith is the author of the *Car Hacker's Handbook* and founder of OpenGarages.org.

Jesse Sowell holds a PhD in technology, management, and policy from MIT's Engineering Systems Division, and will be joining Stanford's Center for International Security and Cooperation (CISAC) as cybersecurity policy fellow in October. His dissertation evaluated common resource management institutions that sustain the integrity of the Internet's routing system, and documented the authoritative institutions these communities have developed for managing information resources such as numbers and routing information.

Richard Stallman launched the free software movement in 1983 and started the development of the GNU operating system (see www.gnu.org) in 1984. (GNU is free software: everyone has the freedom to copy it and redistribute it, with or without changes. The GNU/Linux system, basically the GNU operating system with Linux added, is used on tens of millions of computers today.) Stallman has received the ACM Grace Hopper Award, a MacArthur Foundation fellowship, the Electronic Frontier Foundation's Pioneer Award, and the Takeda Award for Social/Economic Betterment, as well as several doctorates honoris causa, and has been inducted into the Internet Hall of Fame.

Amie Stepanovich is an expert in domestic surveillance, cybersecurity, and privacy law. At Access Now, Amie leads projects on digital due process and responds to threats at the intersection of human rights and communications surveillance.

Lisha Sterling is the executive director at Geeks Without Bounds, a nonprofit organization that supports open-source humanitarian projects through hackathons and an accelerator program. She is listed in the P2P Foundation's list of "100 Women Co-Creating the Peer-To-Peer Society." She has been a software developer for over 20 years. She brings that experience together with her formal education in Latin American studies and early work experience in international aid and refugee support to help engineers and those who work in crisis response build common languages for working on a wide range of challenges.

Stoppay joined Radio Statler during The Next HOPE (2010) and has since managed the website. He works best under pressure and with little sleep, creating the site and content on the fly. He is known to do on-air interviews from time to time and plays the devil's advocate regardless of his opinion on the subject.

Kit Stubbs is a non-binary/queer/pansexual roboticist, maker, and entrepreneur who's more interested in people than in technology. Kit earned their PhD in robotics from Carnegie Mellon University in 2008 and later launched the Effing Foundation for Sex-Positivity (effing.org), a nonprofit whose mission is to reduce sexual shame by fostering sex-positive artists and educators. They blog about technological empowerment for sexuality and pleasure, including their experiences and creations, at toymakerproject.com. Kit also organizes teasecraft-boston, a meetup group for sex/kink-positive makers (teasecraft.com). They are excited to be back at HOPE after presenting "The Sex Geek as Culture Hacker" at HOPE X. You can also see Kit's work featured in Johannes Grenzfurthner's film *Traceroute.*

TechDarko is an information security engineer in San Francisco and technology polymath. Created in the lab of a mad scientist in New Jersey, he craves pizza, bagels, diners, and people with brains. He dabbles in emergency medicine, amateur radio, professional audio and lighting, electronics, broadcast radio, and helping nonprofits adopt new technology. A man of uncommon tastes, he is best bribed/thanked with good ciders and mead. You can often find him at HOPE by hurting yourself (seriously - don't interrupt his drinking time). TechDarko is a founding member of Radio Statler.

Phillip Torrone is partner at Adafruit, helping to manage the day-to-day challenges of running a factory in New York City. He was previously senior editor at *Make Magazine,* producing the *Make* blog, creating the *Make* video series, and working on the Maker Shed online store and Maker Faire. He was also senior editor at *Popular Science,* how-to editor at Engadget, and founder of Hackaday.com.

Since 1990, **TProphet** has been a regular writer, speaker, and columnist for *2600: The Hacker Quarterly.* He believes that most of the world's problems can be solved when people talk together on the phone.

Alexander Urbelis, CEO of Black Chambers Inc., an information security consultancy, and a partner in the Blackstone Law Group, is an attorney who has also been part of the Infosec community for more than 20 years, and a part of *2600* in one way or another since 1994. Over the years, Alex has worked for the U.S. Army, Dartmouth College's Institute for Security Technology Studies (a federally funded cybersecurity and counterterrorism research center), the CIA, the U.S. Court of Appeals for the Armed Forces, the international law firm of Steptoe and Johnson, and as information security counsel and chief compliance officer of one of the world's largest luxury conglomerates. Alex holds a BA, summa cum laude, in philosophy from Stony Brook University, a JD, magna cum laude, from Vermont Law School, and the BCL from New College, Oxford University.

Filippo Valsorda is a systems and cryptography engineer at CloudFlare, where he kicked DNSSEC until it became something deployable. Nevertheless, he's probably best known for making popular online vulnerability tests, including the original Heartbleed test. He's really supposed to implement cryptosystems, not break them, but you know how it is.

Sacha van Geffen is the managing director of Greenhost, a Dutch web hosting company dedicated to providing a sustainable Internet infrastructure and protecting digital civil rights. He is co-author of *Basic Internet Security* (a manual primarily for journalists on securing online communication) and a participant in the broader effort to build more secure systems.

Roy Wattanasin is an adjunct faculty at Brandeis University in both the health and medical informatics and information security graduate programs. He is also a health care information security professional. Roy spends most of his time leading, teaching, and developing information security programs, finding vulnerabilities, performing incident response, and working on many projects.

In October 2009, over three years before Snowden confirmed it, **Marcy Wheeler** guessed that parts of President Bush's Stellar Wind program had been moved to FISA pen registers and Section 215. She stupidly allowed herself to be persuaded to stop pursuing that guess - a mistake she hopes to avoid in the future. She continues to find the hidden traces of surveillance programs in public documents and government obfuscation, both at her own site, emptywheel.net, as well as at other outlets. Marcy has a PhD in comparative literature and lives in Grand Rapids, Michigan.

David Williams-King grew up in the Canadian countryside in a solar-powered house, and is now a computer science PhD student at Columbia University. He researches randomization-based security techniques and maintains an interest in graphics, compilers, and speech recognition. David is privileged to have taught C++ with Bjarne Stroustrup, and proud to have once received an award at the ACM Turing Award ceremony.

Alex Winter entered show business as a child actor on Broadway and came to prominence in movies such as Warner Brothers' hit *The Lost Boys* and the wildly popular *Bill and Ted* franchise. He has directed three narrative features: cult classic *Freaked* for 20th Century Fox; *Fever* for Lionsgate, which screened at Cannes; and *Smosh: The Movie,* which opened in 2015 as the number one comedy on iTunes. Winter's TV credits range from MTV's *The Idiot Box* to Emmy-nominated work for Cartoon Network, as well as numerous commercials and music videos. Alex is the recipient of the Charles Guggenheim award for his directing work. His VH1 rock doc *Downloaded* has earned nationwide critical acclaim at theatrical and festival screenings. His latest award-winning documentary *Deep Web* had a critically acclaimed world premiere at SXSW and a broadcast premiere in the U.S. on the Epix network. The film opened as the number one documentary on iTunes in September 2015. Alex is now making the definitive documentary on Frank Zappa, which set the record as the highest funded documentary in Kickstarter history.

XioNYC (né NeoAmsterdam): The programmer that isn't, master of the splice block, #FailFactory survivor, third eye for the blind, AMD VIZ Vet; F/S. Have OLPC XO-1 will travel; en_US, es_AR, ñyc2600; 0113-1141, 0194-357X, 0-287222-3, 0-74471-01720-1, 0-201-37937-6, 0-8143-3203-X.

Johnny Xmas is a penetration tester for RedLegg, based in Chicago, and has been speaking internationally on the topics of information security, career advancement, and social engineering for nearly 15 years, both in and very far outside of the information security community. His infamous mixture of humor, raw sincerity, and honest love of people lead to hilarious - but at their core serious - discussions revolving around our inherent desire to get in our own way.

Tamara Yadao, multimedia artist and performer, works with conceptual methods of sound-making, music-making, and video by repurposing new and antiquated forms of technology including gaming hardware and software, radios, and transmitters. She also writes chip music under the moniker Corset Lore and has a release on Philly chip music imprint 8static, while also appearing on compilations from 8bitpeoples and Pxl-Win. She is delighted to be curating and coordinating the live music concerts for The Eleventh HOPE.

John Young has operated cryptome.org since 1996 along with his wife, Deborah Natsios. The site publishes information about freedom of expression, privacy, cryptography, dual-use technologies, national security, intelligence, and government secrecy.

Stefan "Sec" Zehl studied computer science and has been working for various companies in the security industry, is a longtime member of the Chaos Computer Club, and is one of the founders of the Munich CCC group. He was part of the team that created the rad1o badge for the Chaos Communication Camp - delivering 4500 broadband SDRs based on the HackRF to the security researcher community.

Lucas Zhao (UrbanHawk) is a 16-year-old lockpicker with a special interest in Chinese locks and an avid collector, with a collection mostly consisting of unusual Chinese-made locks. He has been dissecting and researching locks since he was ten years of age, and has a fairly comprehensive knowledge of all things related to locks. Lucas loves to talk endlessly about his lock interests to anyone who will listen, much to the annoyance of his friends. He also knows too much about other random topics such as elevators and the Metro-North Railroad, which his friends now avoid in order to keep him from talking endlessly about those as well.

Yan Zhu is a security software engineer and friend of Chelsea Manning.

WORKSHOPS

(on 6th floor unless otherwise designated)

3D Modeling with Fusion 360

Come one, come all and learn to model with Autodesk's newest 3D design tool: Fusion 360, a cloud-enabled 3D CAD (Computer Aided Design), CAM (Computer Aided Machining), and CAE (Computer Aided Engineering) tool that makes product design faster and easier than ever before. Fusion 360 is an innovative program that combines the ability to parametric and free form model, run simulations, and edit and review with a group over the cloud. Plus it's great for beginner modelers and experienced product designers alike! Come with your ideas, a ready-to-learn mind, and the free trial version of Fusion 360 downloaded on your laptop and this workshop will take it from there!
Saturday 1530-1730 Budapest

Amateur Radio License Exam

You can take the Amateur Radio exam at The Eleventh HOPE! All levels of tests are offered.
Sunday 1300-1500 Paris

Anti-Surveillance and Privacy Policy

This is a workshop, as well as an extended Q&A associated with the "Spy Hard with a Vengeance" talk.
Sunday 1630-1730 Budapest

Arduino for Total Newbies

You've probably heard lots about Arduino. But if you don't know what it is, or how you can use it to do all sorts of cool things, then this fun and easy workshop is for you. As an example project, you'll be creating a TV-B-Gone remote control out of an Arduino you can take home with you. *(Materials fee: $35) Optional: bring your laptop if you'd like it set up for playing with Arduino.*
Saturday 1530-1900 Hardware Hacking Area (Mezzanine)

Crypto Party

Following Comet Crowbar's talk "How to Start A Crypto Party," you can join her for this beginner's introduction on how to resist surveillance by embracing tools for encryption and how to be anonymous online. She will cover strong passwords, GPG encryption, and explain what a "keypair" is, along with Signal, Tor, and other common tools. This will be half a presentation, half hands-on doing stuff on your computer/devices (*bring them if you have them!*).
Friday 1930-2130 Paris

Cyber Deception: Hunting Advanced Attacks with MazeRunner

During this workshop, attendees will learn about MazeRunner, Cymmetria's free cyber deception general use tool being released for the first time. They will be able to set up deception across environments that will be composed of decoys (real virtual machines that can be Linux/Windows systems), configure these machines with different network protocols and content to make them look like anything to deceive a hacker, and lastly create the connections and credentials to these configurations to deploy to the endpoints, thereby creating a complete layer of deception to lead an attacker. Next, you will be shown how to use the alerts and forensics gathered in order to enable automatic mitigation of threats and enrich your threat intel efforts. *Optional: bring your laptop with KVM (Linux) OR VMWare (Windows).*
Sunday 1000-1200 Paris

DIYSECT: film screening of *Biotinkering for the Web*

DIYSECT is a documentary web series on biohacking and bioart, focusing on the social, political, and philosophical aspects of biotechnology. Initiated in 2013, *DIYSECT* has released five episodes and gathered interviews from over 60 biohackers, bioartists, synthetic biologists, writers, and curators. At The Eleventh HOPE, there will be a screening of all five episodes back-to-back: 1) Learning in Public, 2) Bioterror and Bioerror, 3) Fear of the Unknown, 4) Genocracy, and 5) Hybrid Practices.
Friday 1400-1600 Paris

Exploit Development

Unexpected input often causes programs to crash. Learn how to develop remote code execution exploits from such crashes. In this workshop, participants will take over a series of real servers using these techniques: shell command injection, ImageMagick exploitation, SQL injection, and buffer overflows with shellcode. Participants need to bring a computer running OS X or Linux in either a real or a virtual machine. A few loaner laptops will be available.

Sunday 1600-1900 Paris

FOIA 101

This workshop will show you how to request a variety of federal agency records using the Freedom of Information Act, the Privacy Act, and Mandatory Declassification Review; and also how to get state and local agency records under similar state laws. The format of a request letter will be illustrated, and there will be a discussion on how to find the right agency and address to send a letter, how to frame the letter to avoid fee problems, what phrases help prompt agencies to disclose the most information, and other requester tools. You will learn how the process of getting electronic records differs from that of getting paper records, and you will hear case studies detailing how public records have been used by journalists, activists, and the general public to better inform our democracy. Becoming familiar with these essential steps streamlines the process and make it simpler for both requesters and the offices from which they are requesting records. This workshop will feature an opportunity to ask questions of the panelists.

Saturday 1900-2000 Paris

FOIA 201: Advanced FOIA Strategies and Tactics

This workshop will review some of the common methods agencies use to deter or deny requests, and how to react constructively so you can get the records you want. Among the aspects that will be discussed are how to fight off improper fees, how to ask for database records, how to negotiate successfully with agency staff, when to narrow a request, and how to best respond when agencies say "you can't have that." You will also learn how to figure out what to ask for and formulate a request so that it is most likely to produce a useful response in a useful data format. Examples will be drawn from the GovernmentAttic.org and MuckRock websites as well as the experience of the panelists. This workshop will feature an opportunity for give and take discussion based on the interest of attendees, and the opportunity to ask questions of the panelists and other participants.

Saturday 2000-2130 Paris

Getting Started with Encrypted Communications

Want to encrypt your email/chat but not sure how to get started? In this beginner-oriented workshop, you'll get hands-on help in getting set up with encrypted email and chat on your laptop, text, talk, and email on your smart phone. Come at the beginning for a short (15 minute) presentation on security basics and *bring your laptop or smart phone* for hands-on help! (If you just want to get set up and go, drop-ins are also welcome!)

Friday 1000-1200 Paris

Holistic Info-Sec for Web Developers

Join Kim Carter for an exploration into an insightful set of steps he has learned, from an architectural, engineering, and penetration testing perspective. Based on the content of Volume 0 and 1 of Kim's new book *Holistic Info-Sec for Web Developers.* Kim will walk through how your Scrum Team can bring the specialized process of penetration testing from the release phase to right up front, augmenting your Scrum process within each and every Sprint using a collection of processes, practices, and tools that have proven their value in the field of information security. Kim will walk us through the SSM threat modeling process with examples in areas such as physical, people, VPS, network, cloud, web applications, etc.

Saturday 1000-1200 Paris

How to Fight an Internet Shutdown

Internet shutdowns pose a terrifying and real threat worldwide. They have become early warning mechanisms for human rights violations during the most critical moment of democracies: elections. In 2015 alone, Access Now recorded nearly 20 shutdowns in a variety of contexts and situations, from the Pacific Ocean to Pakistan to the Democratic Republic of the Congo. Even the U.S. has a mysterious "kill switch" rule on the books called Standard Operating Procedure 303 that could allow the government to shut down the net. Shutdowns harm innovation, stymie local economies (banks alone lost an estimated $22.6 million during an April shutdown in Kashmir, India), and block the use of emergency services. Come join this workshop as a real Internet shutdown is simulated through interactive role play. What can you do? What should companies do? What about telcos and governments? Find out how you can make a difference.

Saturday 1630-1830 Paris

Intro to Ham Radio:
What You Need to Know Now to Start Tomorrow

Whether you're interested in DIY electronics, digital communications, or technology in general, you'll find something to interest you in amateur radio. This workshop will cover some basics of the amateur radio service (how to get a license, different types of equipment, operating modes, etc.), highlight some of the most interesting developments, and also offer exam preparation resources and discussion for the amateur radio exam sessions being held on Sunday. Stop by to find out how to get involved in amateur radio, and also leave with enough materials to cram for the exam Sunday so you can get on the air! *Materials/equipment: None required, except for your choice of device for accessing documents online or via a USB drive.*

Friday 1200-1300 Paris

Open Source Estrogen

Open Source Estrogen explores the various ways that estrogen performs a molecular colonization in our society, bodies, and ecosystems. Estrogen is the most ancient of sex hormones. Therefore the mutagenic effects of environmental (xeno) estrogens disrupt species across all animal taxa, including humans. In response to our collective mutagenesis, the workshop uses DIY/DIWO laboratory tools and protocols for detecting and extracting xeno-estrogens. Examples include solid phase extraction with cigarette filters, wine-bottle

column chromatography, and beer yeast biosensors. This workshop will explore the social, ethical, and environmental implications of estrogen deregulation. A 45-minute talk will be given at the beginning, followed by the workshop. *Materials fee: $10*
Friday 1600-1900 Paris

The Next Billion Certificates: Let's Encrypt and Scaling the Web PKI

Let's Encrypt is a free and automated certificate authority. If you're developing a client to integrate with Let's Encrypt or trying to deploy Let's Encrypt certificates at scale, come to this workshop to discuss best practices and work through any issues. *Optional: bring your laptop.*
Saturday 1200-1300 Paris

Pop-Up Plant Lab

A hands-on plant tissue culture pop-up lab catering to the curious but inexperienced, with a focus on teaching the technical and physical manipulations necessary to do plant tissue culture. Students will be instructed on how to dissect and plate leaf tissue of freshly sown tobacco leaves growing in sterile conditions onto media with plant growth regulators which will induce somatic embryogenesis or "babies from the body." All plant cells can be reprogrammed using chemical queues such that near-infinite clones of the original plant can be produced. This technology is used in industrial-scale production of ornamental plants but requires minimal overhead if approached creatively. Using over the counter vessels and easily made lab equipment, you too can clone your own army of plants and you'll learn how here!
Various Times - Biohacking Area (Mezzanine)

Violent Python

Even if you have never programmed before, you can quickly and easily learn how to make custom hacking tools in Python. In hands-on projects, participants will create tools and hack into test systems, including: port scanning, login brute-forcing, port knocking, cracking password hashes, ARP spoofing, layer 7 DoS attacks, and sneaking malicious code past antivirus products. Participants need to bring a computer running OS X or Linux in either a real or a virtual machine. A few loaner laptops will be available.
Saturday 1300-1600 Paris

6TH FLOOR SCHEDULE

FRIDAY

	Paris
1000-1200	Getting Started with Encrypted Communications
1200-1300	Intro to Ham Radio: What You Need to Know Now to Start Tomorrow
1400-1600	*DIYSECT:* film screening of *Biotinkering for the Web*
1600-1900	Open Source Estrogen
1930-2130	Crypto Party
	Budapest
1100-0100	Further Discussion Following 18th Floor Talks

SATURDAY

	Paris
1000-1200	Holistic Info-Sec for Web Developers
1200-1300	The Next Billion Certificates: Let's Encrypt and Scaling the Web PKI
1300-1600	Violent Python
1630-1830	How to Fight an Internet Shutdown
1900-2000	FOIA 101
2000-2130	FOIA 201: Advanced FOIA Strategies and Tactics
	Budapest
1100-1530	Further Discussion Following 18th Floor Talks
1530-1730	3D Modeling with Fusion 360
1730-0100	Further Discussion Following 18th Floor Talks

SUNDAY

	Paris
1000-1200	Cyber Deception: Hunting Advanced Attacks with MazeRunner
1300-1500	Amateur Radio License Exam
1600-1900	Exploit Development
	Budapest
1100-1630	Further Discussion Following 18th Floor Talks
1630-1730	Anti-Surveillance and Privacy Policy
1730-1900	Further Discussion Following 18th Floor Talks

WHAT OUR ROOM NAMES MEAN

Hedy Lamarr was a film actress and inventor. Among her inventions are an improved traffic light and a tablet that dissolved in water to make a carbonated drink. In 1942, Lamarr and composer George Antheil received a patent for their Secrecy Communication System, which was designed to prevent jamming in radio-controlled torpedoes. After the introduction of the transistor, this frequency-hopping invention led to today's spread-spectrum technology including GPS, Bluetooth, and CDMA.

Emmy Noether was a mathematician with groundbreaking contributions to abstract algebra and theoretical physics. Having been described as the most important woman in the history of mathematics, she developed the theories of rings, fields, and algebras. Noether's theorem resolved a paradox in general relativity, but it also is a general tool for deriving conserved quantities from symmetries.

Elizebeth Friedman has been called "Amer***i***ca's first female cryptanalyst" and is a pioneer of U.S. cryptology. It was her love of Shakespeare and efforts to ***d***ebunk the myth that Francis Bacon had wr***i***tten some portion of Shakespeare's bo***d***y of work that ultimately led to her cou***n***terintelligence w***o***rk for ***t***he Navy and then the Treasury Department ***w***here she helped to b***r***ing sc***i***en***t***ific and advanc***e***d ma***t***hematical processes into t***h***e fi***e***ld. After World War II, she ***p***roceeded to contract for the Internationa***l*** Monetary Fund where she created their communic***a***tions securit***y*** sy***s***tem.

Erna Hoover is a mathematician who revolutionized modern communication with her invention of a computerized telephone switching method. Receiving one of the very first software patents, this invention provided a way to prioritize incoming calls to prevent the system from overloading during peak usage. Thanks to Hoover, the lines are not full of busy signals and dropped calls.

ATTRACTIONS & RESOURCES

***2600* Store:** In addition to the efforts and talents of our many awesome volunteers, these conferences are made possible through the continued support of *2600 Magazine*. Please show *your* support and keep *2600* alive, which will also help keep HOPE alive. The *2600* store is on the 18th floor in the main corridor between the speaking areas and is stocked with back issues, calendars, t-shirts, hoodies, DVDs, books, caps, and lots more.
Friday through Sunday - 18th Floor

Amateur Radio Special Event Station W2H & 70cm Repeater: If you're an amateur "ham" radio operator, bring your handie-talkie to communicate with the many hams at HOPE and keep up with what's happening. Visit Special Event Station W2H on the 18th floor and operate on several HF/UHF/VHF bands to communicate with hams around the globe sans infrastructure - and even with the International Space Station (ISS) as it passes over. A 70cm repeater will have an input of 442.875 MHz and output of 447.875 MHz (PL 167.9 Hz). Simplex operations on 2M and 70cm will be on 147.545 MHz and 433.545 MHz with PL 77.0 (XB).
Friday through Sunday - 18th Floor (near Lamarr entrance)

Art: The bleeding edge of art and the bleeding edge of technology are often one and the same. Simultaneously, art allows us to process the darker aspects of tech, like three letter agencies surveilling every move. The art at The Eleventh Hope covers these extremes.
Friday through Sunday - Mezzanine

Club-Mate: The hacker community in Germany became thoroughly addicted to this unique, carbonated, caffeinated beverage made from genuine yerba mate leaves. It gives you lots of energy, is lower in sugar than sodas, and doesn't hit you with that "energy drink crash" when you stop drinking it. Club-Mate was first introduced in the U.S. in 2008 at The Last HOPE, where it was met with great enthusiasm by the American hacker community. Since then, we've supplied hackerspaces and rock stars with many pallets of the stuff. Get yourself a cold half-liter bottle of Club-Mate (courtesy of our new Club-Mate freezer) or pick up an entire case, and stay up and energized throughout The Eleventh HOPE.
Friday through Sunday - Mezzanine

Concerts: Friday and Saturday nights, grab a Club-Mate, come down to the atrium, and party while hacker DJs mix, spin, bend, mod, synth, sample, and twiddle bits and beats all night long! Details on who's playing and when are being posted throughout the conference, along with ways that non-HOPE attendees can be a part of the fun.
Friday, Saturday nights - First Floor

Fourth Track: In the HOPE tradition of free speech, this forum is for unscheduled speakers to present a talk for one hour on any topic they like. The Hoover room on the 18th floor will be available starting Friday morning. The room accommodates about 60 people, and the HOPE Wi-Fi will be accessible there. AC power outlets are available, but no audio/video/projector is available unless you bring one. Speaking slots are 50-55 minutes. You can sign up at the InfoDesk in the Mezzanine on a first-come basis. The schedule will be posted outside the room.
Friday through Sunday - Hoover

Hackers Got Talent: Do you have a cool hack? This is your chance to share it with a whole bunch of other hackers. Hacks will be judged by a combination of panelists and audience. First place wins a valuable prize!
Saturday Night at Midnight - Noether

Hackerspace Village: It's like an outdoor hacker camp village, but inside the HOtel PEnnsylvania. The Hackerspace Village has their own electronics workshop, project space, and social area. Members of hackerspaces and the DIY community from around the world will host informal classes, workshops, demos, giveaways, and other events throughout The Eleventh HOPE. Stop by and meet other interesting people who hack around the world. This is how countless projects are conceived and started.
Friday through Sunday - Mezzanine

Hammock Lounge: Hammocks with Wi-Fi - yes, HOPE sets up a bunch of freestanding hammocks for you to relax and unwind on after many hours of hacking and geeking out. *Warning: these are set to auto-flip after one hour to prevent lingering for too long.*
Friday through Sunday - Mezzanine

InfoDesk: Got a question about anything at The Eleventh HOPE? Stop by the InfoDesk, where the helpful and knowledgeable radio-equipped InfoDesk staff can instantly reach dozens of HOPE staffers and get a quick answer about nearly anything going on. You can even get some good info about local NYC eating and drinking establishments.
Friday through Sunday - Mezzanine

Learn to Solder: A large variety of way cool kits are available, all designed for total beginners to complete successfully - and intriguing enough for the total hardware geek. *Materials cost $10 to $30, depending on the kit.*
Friday through Sunday - Hardware Hacking Area (Mezzanine)

Lockpick Village: Want to tinker with locks and tools the likes of which you've only seen in movies featuring cat burglars, spies, and secret agents? Then come to the Lockpick Village to learn hands-on how the fundamental hardware of physical security operates and how it can be compromised. Experts are on hand to demonstrate - and plenty of locks, picks, shims, and other devices are available.
Friday through Sunday - Mezzanine

Meta Mate Club: In the world outside hacker conferences, we are constantly connected online. This is an invitation to sit down and connect with a mate.... Sharing a mate is more than sipping a tea and the members of this club want to infuse the conference in a new dimension loaded with theobromine, antioxidents, and caffeine from the wild forests produced in an autonomous way. All Hackers On Planet Earth are welcome to drop in on the Mate Space, learn how to make a mate, and collaborate and connect.
Friday through Sunday - Meta Mate Club (Mezzanine)

Midnight Movies:
Friday: *Deep Web* - documentary covering the trial of Ross Ulbricht and chronicling events surrounding Silk Road, Bitcoin, and the politics of the dark web. Introduced by director Alex Winter.
Saturday: *Citizenfour* - the Academy Award winning documentary from Laura Poitras on the early days of the Edward Snowden revelations and the ensuing NSA spying scandal. Look for footage from HOPE Number Nine!
Friday and Saturday at Midnight - Lamarr

Network: The Eleventh HOPE is one of the most Internet-connected events in the country. There is ample wired and wireless connectivity throughout the conference, specifically on floors 1, 2, 6, and 18. And when we say fast (which we are saying now), we mean it. We took last conference's 10 gigabit connection and turned it up to 11. Look for TheEleventhHOPE wireless network and visit https://noc.hope.net for all sorts of important updates. Also, the NOCNOC is where folks can check in server equipment, knowing it will be connected and locked securely in our cage.

Open Microphone: In addition to the ongoing fourth track, we now have a way you can express yourself to the entire HOPE crowd beginning at midnight on Friday night. It's kind of like lightning talks except with much longer lightning. You'll have up to 15 minutes to say your piece and make your points. (You can even sing a song if you wish - it's an open microphone, after all.) Sign up at the InfoDesk on Friday and you will be called upon in the order that you signed up.
Friday Night at Midnight - Noether

Phonehenge: In ancient times hundreds of years before the dawn of history, there were telephones for communications. Come uncover the secrets of Phonehenge at The Eleventh HOPE.
Friday through Sunday - Mezzanine

Press Room: The Eleventh HOPE is pleased to host world-class and independent journalists from around the world to report on the unique happenings at this truly historic event. Large and small news media outlets, radio and television stations and networks, newspapers, magazines, and numerous online publications will all be covering The Eleventh HOPE. Journalists can take advantage of a quiet(er) space near the workshops and follow-up sessions that are taking place on the 6th floor. Here it will be possible to conduct one-on-one interviews with HOPE speakers, panelists, workshop presenters, project managers, organizers, volunteers, and others. Journalists - get your scoops here!
Friday through Sunday - London (6th Floor)

Radio Statler: Do you have something to say? Do you want to help bring HOPE to the world? Then stop by Radio Statler on the Mezzanine and join them as they broadcast original programming and expanded conference content to the wide reaches of the Internet. Radio Statler is HOPE's 24-hour live streaming audio station, named after one of the hotel's other names from years past: the Hotel Statler. Radio Statler features original content such as interviews with HOPE speakers, workshop presenters, artists, musicians, exhibitors, staff, and attendees. Sign up to do your own show, help out with someone else's, or just sit in on some in-depth interviews and roundtable discussions. Know someone who can't make it to the conference? Tell them to listen to the Radio Statler audio stream at radio.hope.net - The Voice Of HOPE!
Friday through Sunday - Mezzanine

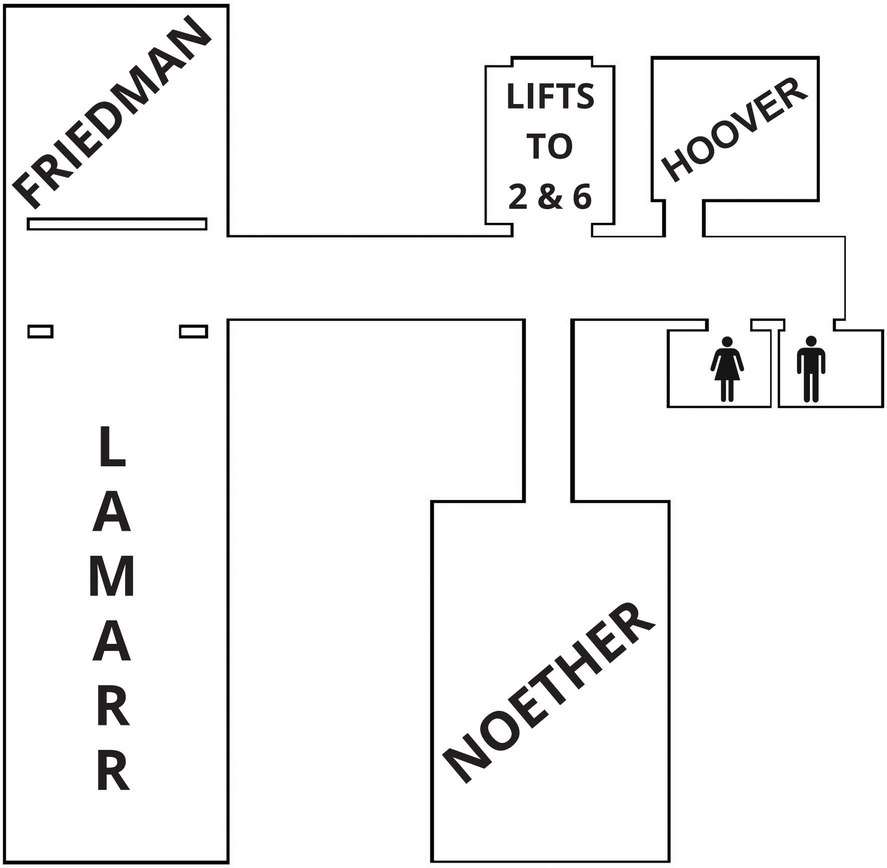
Retrotech: The best old school hacks used the hardware that was available and took it to 11. Without hardware like this, the Internet as we know it wouldn't have been formed. Take a look at some of the hardware which was greenwired, reworked, and hand-built to do the impossible (including the original Zenith used to edit the first issues of *2600!*).
Saturday, Sunday - Mezzanine

Security/First Aid: Lose your mobile phone or wallet? It's way more likely to be turned in at The Eleventh HOPE security desk than outside on the street! There are *no* security goons at The Eleventh HOPE. Our internal security staff are all hackers, all highly professional, and they do a great job keeping you (and things) safe and under control in a crowd of thousands - all while keeping a friendly, low profile.
Friday through Sunday - Mezzanine

Segway Human Transporters: In 2001, inventor and entrepreneur Dean Kamen unveiled the long-secret project some visionaries speculated could change the world. While it didn't really do that, the Segway Human Transporter (codename:Ginger) is a pretty impressive feat of engineering that still fascinates many hackers. Phosphate-based lithium-ion batteries, bi-directional servo drive motors, multiple microcontrollers, tilt sensors, accelerometers, five gyroscopes, and an inertial navigation control system that seems to read your mind make this unique transportation machine worth trying out. The Eleventh HOPE indoor Segway track and keys to the machines are yours to exploit!
Friday through Sunday - Mezzanine

Vendor Area: At every HOPE conference, there's a nice group of vendors who offer stuff of interest to hackers. Books, electronic kits, t-shirts, lockpick sets and tools, and all kinds of other stuff you might not find anywhere else. Support our vendors who help make HOPE possible. We donate vendor tables to selected non-profits who support our community, such as the Electronic Frontier Foundation (EFF), American Civil Liberties Union (ACLU), Freedom of the Press Foundation, and others. They deserve our support for all of the vitally important work they do for our community and for everyone else.
Friday through Sunday - Mezzanine

EIGHTEENTH FLOOR



Flip to the inside front cover
for second floor information

Come and Visit Our Vendors on the Mezzanine

American Civil Liberties Union

BeeLine Reader

Black Cross

Calyx Institute

Courage Foundation

Electronic Frontier Foundation

The FreeBSD Foundation

Freedom of the Press Foundation

Free Software Foundation

Hackaday

HackerStickers.com

Lime Microsystems

No Starch Press

OR Books

OWASP

PreEmptive Solutions

Privoro

Security Snobs

SEREPICK

Soylent

Sparkle Labs

Tesla Science Center at Wardenclyffe

ThinkPenguin

A Very Special Thanks to Our Generous Sponsors

aruba

a Hewlett Packard
Enterprise company

THE CBD

cryptobiz.directory

HE HURRICANE ELECTRIC
INTERNET SERVICES